Using NetShield

MCAFEE

Document Release NS.22

Table of Contents

Chapter 4 Scanning 33

Chapter 5 Notification and Reporting 44

Chapter 6 Security 53

Chapter 1 Introducing NetShield

Thank you for purchasing NetShield™, McAfee’s advanced anti-virus solution for Novell NetWare file servers. NetShield combines McAfee’s award-winning proprietary Code Trace™ and Code Matrix™ virus scanning technologies with file server management capabilities to effectively minimize and manage the virus threat within Novell networks. Because NetShield is a Novell NetWare Loadable Module (NLM), McAfee can enhance NetWare’s security services without jeopardizing file server operation. NetShield becomes a part of NetWare services, offering real-time virus security to NetWare 3.11, 3.12, 4.X, and SFT III systems.

NetShield efficiently scans in real-time for virus infected files transmitted to and from the file server, preventing the spread of viruses throughout the network. In addition, NetShield scans for viruses hidden within the file server itself. Once an infected file is detected, it is automatically logged and either isolated or deleted. Further, NetShield can be configured to check for any file modifications as well as enhance NetWare’s access security. Teamed with McAfee’s VirusScan, the industry’s top-rated DOS, Windows, and OS/2 desktop anti-virus solution, NetShield offers a significant barrier against the damage to data and productivity that viruses may cause within a network environment.

Overview

NetShield’s flexibility allows you to configure virus protection to your particular network. Use this task list as a road map for applying the information in this manual to your network:

- **Task 1: Before Installation.** Before getting started, ensure that you have everything you need to install NetShield. If you have downloaded NetShield, compare the required NetShield files with the check list found within the associated “read me” file. Additional patches are required for NetWare 3.11 and 3.12 installations; copy the NetShield files to the server SYS\SYSTEM directory.
- **Task 2: Installation.** You will be installing the NetShield NLM on every file server at your site. Because NetShield is licensed per file server, refer to your license agreement in order to ensure proper legal compliance. Refer to Chapter 2, “Installation,” for more information.

NOTE: If you use a bootable floppy diskette to start your file server, ensure that the boot diskette is clean of any viruses. The documentation for VirusScan, a McAfee desktop anti-virus solution, describes a procedure for creating a clean bootable diskette. Refer to “McAfee Support” later in this chapter for more information about obtaining VirusScan.

- **Task 3: Scanning Configuration.** McAfee recommends that you begin with an immediate scan of your network to detect any present viruses. Next, set NetShield to run scans during periods of low network traffic using the “periodic scanning” settings. This will protect your network from infection without interfering with network activity. In addition, you should set NetShield to scan all files transferred to and from the file server, using the “on-access” scanning settings. On-access scanning provides real-time protection against the transmission of infected files throughout your network. Finally, have NetShield move infected files to a “quarantine” directory for later inspection. Refer to Chapter 4, “Scanning,” for details.
- **Task 4: Notification and Reporting Configuration.** NetShield can inform you when a virus is found, both through alert messages to selected users and by recording the information in a log file. We recommend that you set up NetShield to log infections in a file and at least notify the network supervisor in order to measure and respond to the virus threat. Refer to Chapter 5, “Notification and Reporting,” for details.
- **Task 5: Updating.** New viruses and strains of existing viruses are being detected every day. McAfee’s virus research team releases a new virus signature file update at least once every month. This update should be installed on your file server to maintain NetShield’s detection ability. When you receive or download an update, install it onto one of your file servers and enable cross-server updating. NetShield will automatically update all the NetShield file servers on the network. Refer to “McAfee Support” later in this chapter and “Cross Server Updating” in Chapter 4, “Scanning” for more information.
- **Task 6: Virus Elimination.** Rather than deleting virus infected files, NetShield can isolate infected files for further analysis and removal. We recommend McAfee’s VirusScan for cleaning virus-infected files. By cleaning infected files you can prevent the loss of important data that can occur when infected files are deleted.

About NetShield

NetShield is an advanced anti-virus solution designed to protect your Novell network from viral infection. Employing McAfee’s patented Code Trace™ and Code Matrix™ virus scanning technologies, NetShield consistently and accurately identifies both known viruses and new viruses, including file, multi-partite, stealth, mutating, polymorphic and encrypted types. NetShield uses the following methods to detect these viruses:

- Known viruses are detected by searching the system for known characteristics (sequences of code) unique to each computer virus and reporting their presence if found. For viruses that encrypt or cipher their codes so that every infection is different, NetShield uses detection algorithms that work by statistical analysis, heuristics, and code disassembly.
- Strains of known viruses are detected by searching for “generic” or “family” virus strings that have been found repeatedly in different viruses. Since virus writers may use older code or programming techniques when writing new viruses, NetShield can use these strings to detect viruses that have not yet been written.
- New or unknown viruses can be detected by comparing files against previously recorded validation data. If a file has been modified, it will no longer match the validation data, and NetShield will report that the file may have become infected. For more information, refer to “Cyclic Redundancy Check Validation” in Chapter 4, “Scanning.”

NetShield offers three methods of scanning: **Immediate scanning**, to perform a scan of your network on demand; **On access scanning**, to prevent infected files from being copied from and/or to a file server; and **Periodic scanning**, to schedule automatic scanning on a specific day and time. If NetShield detects infected files, it can **delete**, **move**, or **ignore** the files. For more information about scanning options and infected file actions, refer to Chapter 4, “Scanning.”

If NetShield discovers infected files on your network, you can also specify its notification actions, alerting one or more users through **console messages**, **network broadcast messages**, **e-mail messages**, or **pager messages**. Scan results can be written to a log file to provide an infection trail for future audits. For more information about notification options and logging, refer to Chapter 5, “Notification and Reporting.”

For networks requiring even greater anti-virus security, NetShield can restrict file server access by specified users, or prevent file server writes by file type or to specified directories. Furthermore, NetShield can grant temporary access to certain files or directories to enable only authorized users to upgrade or install software. For more information regarding network security, refer to Chapter 6, “Security.”

NetShield's Features

NetShield offers the following features:

- **NetWare certification** on 3.X and 4.X NetWare file servers, including NetWare Directory Services (NDS) support
- **Windows console** provides user-friendly graphic interface
- **On access scanning** to monitor inbound and outbound files for viruses
- **On demand scanning** to immediately identify infected files within the file server
- **Periodic scanning** allows scheduled scans every day, week or month
- **Predefined action on detection:** ignore, delete or move infected files
- **Incident notification options** including administrator's console, network broadcast, e-mail via Global Message Handling Services (GMHS) and numeric pager
- **Automatic cross-server updating** to synchronize the most current detection capabilities among file servers
- **Cyclic Redundancy Check validation** to identify file modifications associated with unknown viruses
- **Write-access administration** restricting and monitoring write attempts by files, file types, directories or users

McAfee Support

For help in using this product, or for more information about McAfee's VirusScan and other products, we invite you to contact McAfee Associates technical support. You can contact us:

McAfee, Inc.

2710 Walsh Avenue

Santa Clara, CA 95051-0963

U.S.A.

Phone	(408) 988-3832

FAX	(408) 970-9727
Hours	6 a.m. to 5 p.m. PST
McAfee BBS	(408) 988-4004 1200 bps to 28,800 bps 8 bits, no parity, 1 stop bit 24 hours, 365 days a year
CompuServe	GO MCAFEE
Internet	support@mcafee.com
America Online	MCAFEE

Before you call

For fast and accurate help, have the following information available when you contact McAfee:

- Product name and version number
- Type and brand of computer, hard disk, and any peripherals
- DOS version
- NetWare version
- Printouts of your AUTOEXEC.NCF and STARTUP.NCF files and a modules list
- A description of the exact problem you are having. Be as specific as possible. If you cannot be at your computer when you call, a printout of the screen will be helpful.

If you are overseas, you can contact a McAfee authorized agent. Agents are located in 50+ countries around the world and provide local sales and support for our software.

Internet Access

The latest versions of McAfee’s anti-virus software are available by anonymous ftp (file transfer protocol) over the Internet from the **ftp.mcafee.com** site. If your domain resolver does not support names, use the IP address 192.187.128.3. Enter **anonymous** or **ftp** as your user ID and your own e-mail address as the password. Programs are located in the **pub/antivirus** directory. If you have questions, send e-mail to **support@mcafee.com.**

You can also find McAfee’s anti-virus software at the SimTel Software Repository at **Oak.Oakland.EDU** in the **simtel/msdos/virus** directory and its associated sites:

wuarchive.wustl.edu(US)

ftp.switch.ch(Switzerland)

ftp.funet.fi(Finland)

src.doc.ic.ac (UK)

archie.au (Australia)

Chapter 2 Installation

Chapter 1 introduced NetShield and many of its features. This chapter provides installation procedures for NetShield.

Overview

NetShield must be installed on every file server you want to be protected. (Since NetShield is licensed per file server, please refer to your license agreement in order to ensure proper legal compliance.) If installing from CD-ROM, use the XCOPY /S command to copy the files into a working directory on your PC. If installing from a BBS release, unzip the files into a working directory on your PC. Begin the install by running SETUP.

Environment

The following criteria must be met in order to run NetShield.

System Requirements

- Novell NetWare 3.X or 4.X, including NetWare Directory Services (NDS) support
- Network Disk Space: 18 MB required, 25 MB recommended
- RAM: Minimum of 718 K free on file server

NOTE: Additional patches are needed for NetWare 3.11 or 3.12 installations (refer to “Novell NetWare 3.11 and 3.12 File Server Requirements” later in this chapter). NetShield is not compatible with NetWare v3.10.

Administrator Console Requirements

- Operating System: DOS 5.0 or greater
- User Interface: Microsoft Windows 3.1X in enhanced mode

- CPU: 386SX or higher
- RAM: 4 MB
- Monitor: VGA or better

Workstation Requirements

- Operating System: DOS 3.3 or greater
- RAM: Minimum of 640 K

Novell NetWare 3.11 and 3.12 File Server Requirements

NetShield requires some NetWare patch files for NetWare 3.11 and 3.12. Use the following recommended versions (in parentheses) or higher:

- A3112.NLM (4.10A)
- AFTER311.NLM (4.10A)
- CLIB.NLM (3.12H)
- MATHLIB.NLM (3.12H)
- MATHLIBC.NLM (3.11H)
- NWSNUT.NLM (4.10G)

NOTE: AIO.NLM and AIOCOMX.NLM are required to use the pager notification option. If you intend to use pager notification on a NetWare file server, Refer to “Enabling Pager Notification” in Chapter 5, “Notification and Reporting,” for more information.

NetShield supplies these patches with the CD-ROM release. For BBS release users, Novell supplies these patches in the LIBUP4.EXE file. To obtain this file

- From Novell, refer to the Novlib Forum on CompuServe, the ftp.novell.com anonymous ftp site on the Internet, or other Novell on-line services.
- From McAfee, download it from the McAfee BBS under File Area “P” (for Patches), or from the mcafee.com ftp site in the pub/patches directory.

Copy these files to the SYS\SYSTEM directory on your NetWare 3.11 or 3.12 file server. (When installing CLIB.NLM, the file server must be downed.)

NOTE: *Do not* install these patches on a NetWare 4.X file server.

Before Installation

To install NetShield, you must:

- Login to the network as a SUPERVISOR or equivalent
- Have a drive mapped to your SYS volume or a search drive
- Have at least 4.8 MB (6.8 MB is suggested) available on the PC that will be running the Windows console for the NetShield program, and at least 2.4 MB (2.6 MB is suggested) available for the On-Line Documentation
- Have at least 1.5 MB (3.5 MB is suggested) available on the file server that will be running the file server NLMs

If you are installing from CD ROM, use the XCOPY /S command to make a working copy of the NetShield distribution CD on your local workstation.

Installing NetShield

Installing NetShield is quick and simple, requiring minimal user input.

Use the following procedure to install NetShield on your network. You can exit the installation at any time by choosing Exit in the lower right corner of the installation screen, or by pressing F3.

NetShield must be installed on every server you want to protect.

NOTE: If you are installing on an SFT III system, be sure to load NetShield from the MS engine.

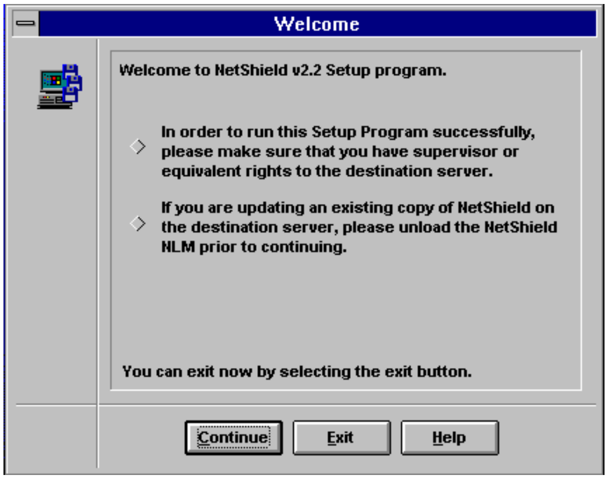
NOTE: If you are currently running a previous version of NetShield, the NLMs must be unloaded from the file server. At the File Server Console, type

```
UNLOAD NETSHLD
```

1. If you are installing from:
   - **CD ROM.** Place the CD in your CD drive.
   - **BBS Release.** Unzip the compressed files to a working directory on your local workstation.
2. Choose File | Run from Program Manager and Browse for the SETUP.EXE file in the appropriate directory, or type SETUP at the DOS prompt.

NOTE: The log file INS220.LOG will be created and placed on your Windows directory. The log file is an ASCII file listing the location of the NetShield installation. The log file also lists any errors that occurred during the installation. If an error that prevents the completion of the install process occurs, the log file be displayed automatically.

3. The Welcome dialog box will be displayed.



Welcome

Welcome to NetShield v2.2 Setup program.

◇ In order to run this Setup Program successfully, please make sure that you have supervisor or equivalent rights to the destination server.

◇ If you are updating an existing copy of NetShield on the destination server, please unload the NetShield NLM prior to continuing.

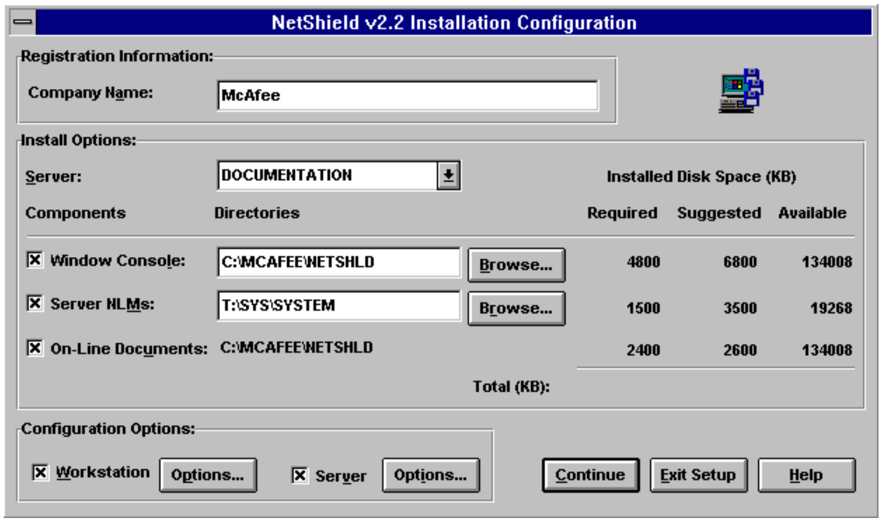
You can exit now by selecting the exit button.

Figure 2-1: Installation Welcome dialog box

Ensure that you have Supervisor or equivalent rights to the destination file server.

4. Choose Continue.

The Installation Configuration dialog box is displayed.



NetShield v2.2 Installation Configuration

Registration Information:

Company Name: McAfee

Install Options:

Server: DOCUMENTATION

Components	Directories	Required	Suggested	Available
☒ Window Console:	C:\MCAFEE\NETSHLD	4800	6800	134008
☒ Server NLMs:	T:\SYS\SYSTEM	1500	3500	19268
☒ On-Line Documents:	C:\MCAFEE\NETSHLD	2400	2600	134008

Installed Disk Space (KB)

Total (KB):

Configuration Options:

☒ Workstation ☒ Server

Figure 2-2: Installation Configuration dialog box

NOTE: The Installation Configuration dialog box displays the required space and the suggested space on the selected volume of the current file server. If there is insufficient space, you must choose a new destination or cancel the installation.

5. Enter your company name in the Company Name text box.

6. Select a file server from the provided drop-down list box.

7. Enter the drive and path that the NetShield Windows Console should be installed to, or choose Browse to locate a path.

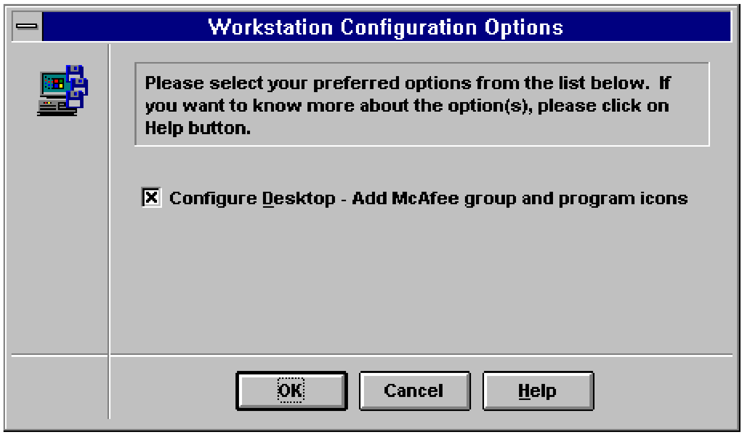
   Verify that the selected drive has sufficient disk space available for this operation.

8. Enter the drive and path that the NetShield Server NLMs should be installed to, or choose Browse to locate a path.

   Verify that the selected drive has sufficient disk space available for this operation.

9. Select the On-Line Documents check box to install the Adobe Acrobat Installer Program (to view NetShield documentation on-line).

10. Choose Workstation Options and select the “Configure Desktop” check box to instruct SETUP to create a McAfee group and program icon.

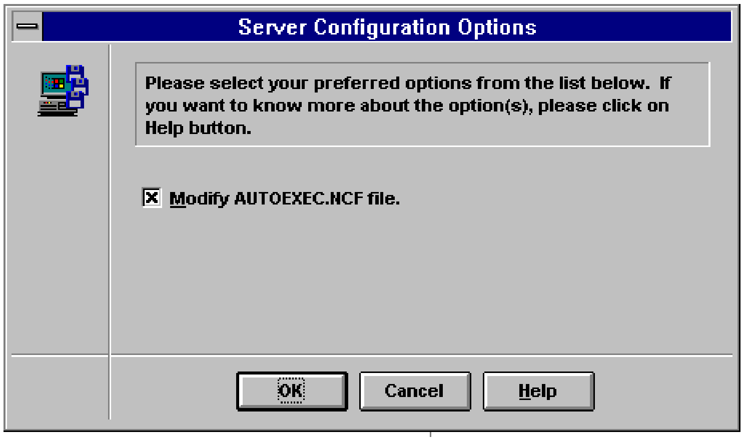


Please select your preferred options from the list below. If you want to know more about the option(s), please click on Help button.

☒ Configure Desktop - Add McAfee group and program icons

Figure 2-3: Workstation Configuration dialog box

11. Choose the Server Options button and select the “Modify AUTOEXEC.NCF” check box to instruct SETUP to modify your file server’s AUTOEXEC.NCF file to automatically load the NetShield NLM at file server startup.



Please select your preferred options from the list below. If you want to know more about the option(s), please click on Help button.

☒ Modify AUTOEXEC.NCF file.

Figure 2-4: Server Configuration dialog box

If you choose to modify AUTOEXEC.NCF, NetShield will add the line “NETSHLD” to your existing AUTOEXEC.NCF file.

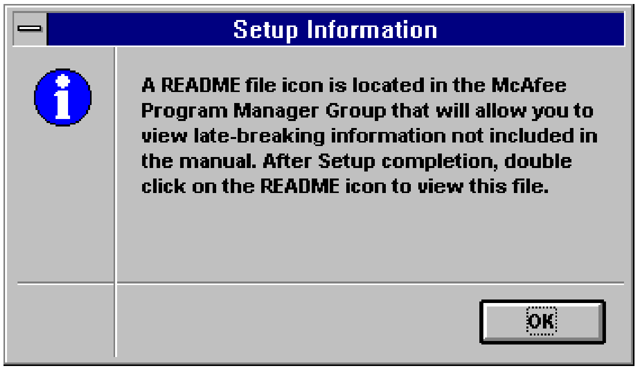
NOTE: If you choose not to modify the AUTOEXEC.NFC file during installation, the NetShield NLM will have to be loaded manually. Refer to “Loading NLMs” for details.

12. Choose Continue.

A dialog box is displayed with a percent completed bar.

If prompted, insert the remaining disks to complete the installation.

The Setup Information dialog box is displayed.



A README file icon is located in the McAfee Program Manager Group that will allow you to view late-breaking information not included in the manual. After Setup completion, double click on the README icon to view this file.

Figure 2-5: Setup Information dialog box

13. Choose OK to indicate that the installation is complete. View the README file for any updated product information.

    NetShield installation is complete. Refer to Chapter 3, “The NetShield Console,” for a description of NetShield’s console and features.

Loading NLMs

NetShield must be loaded on the File Server Console. To load the NetShield NLM, at the file server type:

```
NETSHLD.NCF
```

NOTE: For NetWare 4.X file servers, ensure that DSAPI.NLM is loaded as well.

If you had the SETUP program modify your AUTOEXEC.NCF file, the NetShield NLM will be loaded every time the file server system console is brought up

NOTE: If NetShield does not exist in your SYS\SYSTEM directory, verify that NETSHLD.NCF or AUTOEXEC.NCF contains a valid reference (i.e. a SEARCH ADD statement) to the current directory.

To unload the NetShield NLM, at the file server type

```
UNLOAD NETSHLD
```

For more information about using the file server, refer to Chapter 7, “The File Server Console.”

Chapter 3 The NetShield Console

Chapter 2 described the NetShield installation and upgrade procedures. This chapter introduces and discusses the NetShield application console.

Overview

After entering NetShield and attaching to a file server (see below), the NetShield Console will be displayed, which includes the menu bar, the tool bar, and the NetShield Configuration window for the file server. The following chapter explains how to navigate through the NetShield console.

Windows Terms

As a Windows application, the NetShield console should be used with a mouse. The table below briefly defines several Windows terms regarding the use of the mouse and product windows.

Term	Description
Button 1	The selection or primary mouse button (usually the left button, but can be switched using the Control Panel).
Cancel	Choose Cancel to exit the current dialog box without saving any of the changes you made in the dialog box or without executing a command you chose in the dialog box.
Choose	Click the mouse button (or use a key combination) on an item to initiate an action. For example, “Choose the VirusScan icon” should be interpreted as a click on the VirusScan icon.
Click	Press the mouse button once.
Double click	Press the mouse button twice in quick succession.
Icon	A graphic representation of an executable or function.
Point	Position the cursor on the screen to rest on the desired item.
Property Page	Windows tab metaphor that locates related information in a single dialog box and allows easy navigation from tab to tab.

Scroll	Use the scroll bars and buttons to move through a list of items.
Select	Mark an item by clicking on it or by highlighting it with either key combinations or the mouse. For example, “Select the Include Path option” should be interpreted as click or highlight the Include Path item.
Spin Control	Arrows that increase or decrease the value displayed in the accompanying text box.

NOTE: The remainder of this manual assumes that you are familiar with Windows. Refer to your Microsoft Windows manual for information on the fundamental operating conventions of the Windows environment.

NetShield Menu Bar

The NetShield console’s menu bar consists of the following menu items: File, Scan, Notification, Security, View, Window and Help. To choose a menu item using your mouse, point to the menu name and click the primary mouse button. To choose a menu using keystrokes, press ALT and the mnemonic (underlined letter). For example, press ALT + F for File.

The menu items and their descriptions are listed in the table below.

Menu	Commands
File	Open, Close, Load Configuration, Save Configuration, Exit
Scan	Volume, On Access, Periodic, CRC Options, Infected Action, Exclude Directories, Cross Server Updating
Notification	Logging, User, Mail, Pager, Console Messages
Security	Security Password, Settings, Edit Master List, Select from Master List, Exclude Files, Monitor for all Users, Monitored Users, Temporary Authorization
View	Log File, Configuration File, Tool Bar, Status Bar
Window	New Window, Cascade, Tile, Arrange Icons
Help	Index, Search, Using Help, Product Support, About NetShield

Holding down the primary mouse button over a menu command displays a description of the command in NetShield’s status bar at the bottom of the console window.

NetShield Tool Bar

When using NetShield with a mouse, NetShield’s tool bar buttons provide an alternative for accessing the most frequently used NetShield functions. The tool bar is shown in Figure 3-1.

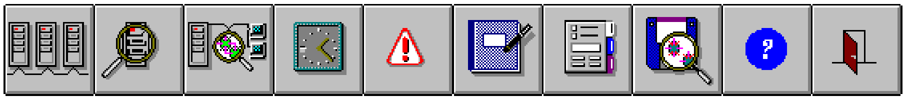
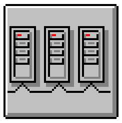
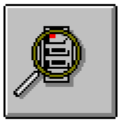
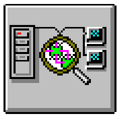
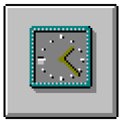
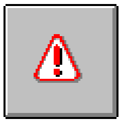
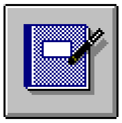


Figure 3-1: The NetShield tool bar

Rather than choosing commands from the drop-down menus, tool bar buttons can be used to perform the same tasks. For example, to begin scanning immediately, you can click on the On Demand Scanning tool bar button, rather than choosing Scan | Volume. The table below lists the tool bar buttons and their descriptions.

Button	Description
	Click here to attach to another file server. For more information, refer to “Attaching to File Servers” later in this chapter.
	Click here to begin an immediate scan of the file server. For more information, refer to Chapter 4, “Scanning.”
	Click here to configure NetShield’s on-access scanning options. NetShield can scan for viruses when files are written to and/or from selected volumes. For more information, refer to Chapter 4, “Scanning.”
	Click here to configure NetShield’s periodic scanning options. NetShield can scan for viruses on a daily, weekly, or monthly basis. For more information, refer to Chapter 4, “Scanning.”
	Click here to configure NetShield’s user notification option, through network broadcast to specified users. For more information, refer to Chapter 5, “Notification and Reporting.”
	Click here to view NetShield’s scan result logs. NetShield can save scan results log in a log file (default name is VIR$LOG.DAT). For more information, refer to Chapter 5, “Notification and Reporting.”

Click here to view a NetShield configuration report file. For more information refer to “Configuration Files” later in this chapter.

Provides access to McAfee VirusScan, desktop anti-virus solution, for additional features such as cleaning.

Launches the Contents help panel. From this panel you can display a list of help topics and subjects. For more information, refer to “NetShield’s Help Facility” later in this chapter.

Click here to exit NetShield.

Using the Keyboard

To use NetShield without a mouse, perform the standard Windows keyboard actions to navigate through the program.

Each menu item on the NetShield menu bar has a keyboard mnemonic. Press the ALT key in combination with the keyboard mnemonic key to choose a menu and cause the menu to drop down. For example, press the ALT + F keys to choose the File menu and display its commands.

Each command also has a keyboard mnemonic. Once the menu is displayed (i.e., “dropped down”), press the keyboard mnemonic of the command you want to choose. For example, from the File menu, press X to choose the Exit command. You can also use the ↑ and ↓ keys to move the highlight to a desired command and press ENTER to select the command.

For detailed information on using a Windows application with the keyboard, refer to your Microsoft Windows documentation.

NOTE: Some NetShield features require the use of a mouse and cannot be accessed with the keyboard.

NetShield's Help Facility

NetShield’s help facility provides on-line assistance for using the NetShield software. To retrieve information quickly about a NetShield feature or procedure, choose Help | Search or click on the Help button from the Tool bar.

Choose the Help | Search command to display an index list of topics. Choose Show Topics to view a list of related topics, or Goto Topic for more information on the selected topic.

NetShield's Help system is written in a standard Windows hypertext format, allowing you to jump from one topic to another by simply choosing topic names from a list. Several buttons display across the top of the Help dialog box allowing you to search for topics and also to view a list of the topics you have visited.

You can access help about a specific operation by clicking on the Help button within a dialog box.

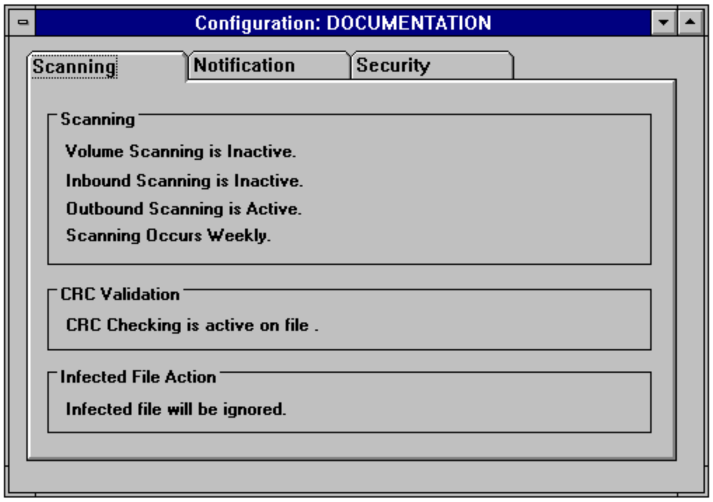
For detailed information on using a Windows help facility, refer to your Microsoft Windows documentation.

The NetShield Configuration Window

The NetShield Configuration window contains three property pages: Scanning, Notification, and Security. The property pages are designed to give you an immediate overview of the properties associated with the attached file server. Each of the property pages are described below.

The Scanning Property Page

The Scanning property page reflects the configuration choices made in the Scan menu.



Scanning

Volume Scanning is Inactive.

Inbound Scanning is Inactive.

Outbound Scanning is Active.

Scanning Occurs Weekly.

CRC Validation

CRC Checking is active on file .

Infected File Action

Infected file will be ignored.

Figure 3-2: The Scanning property page

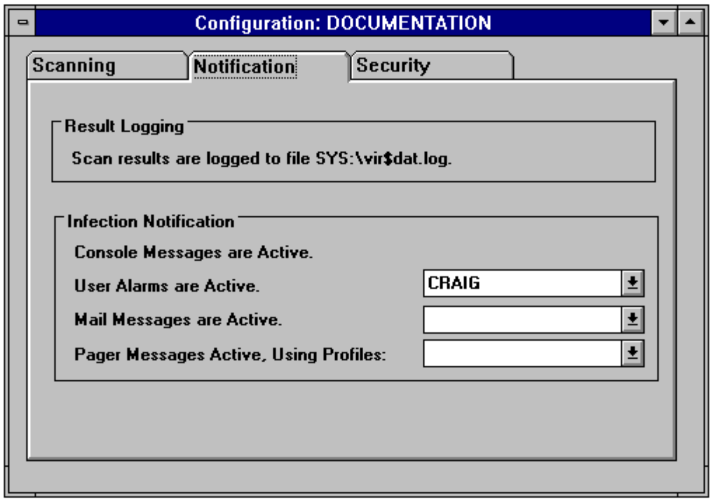
The table below lists the group boxes and fields displayed in the Scanning property page, the associated menu commands and the resulting dialog boxes.

Field	Menu Command	Dialog Box
Scanning		
Volume Scanning	Scan | Volume	Select Volume
Inbound Scanning	Scan | On Access	Access Scanning Options
Outbound Scanning	Scan | On Access	Access Scanning Options
Periodic Scanning	Scan | Periodic	Periodic Scanning Options
CRC	Scan | CRC Options	CRC Options
Infected File Action	Scan | Infected Action	Infected Action

For more information about scanning, refer to Chapter 4, "Scanning."

The Notification Property Page

The Notification property page reflects the configuration choices made in the Notification menu.



Result Logging

Scan results are logged to file SYS:\vir$dat.log.

Infection Notification

Console Messages are Active.

User Alarms are Active. CRAIG

Mail Messages are Active.

Pager Messages Active, Using Profiles:

Figure 3-3: The Notification property page

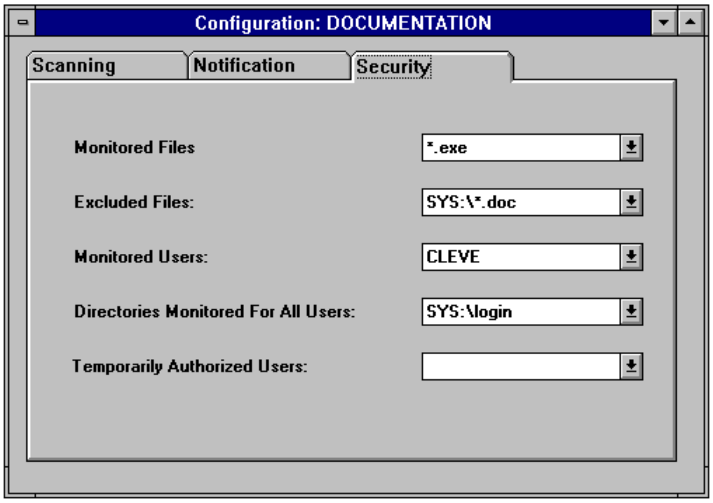
The table below lists the group boxes and fields displayed in the Notification property page, the associated menu commands and the resulting dialog boxes.

Field	Menu Command	Dialog Box
Result Logging	Notification | Logging	Scan Log Settings
Infection Notification		
Console Messages	Notification | Console Messages	Toggle menu item
Mail Messages	Notification | Mail	Mail Notification
Pager Messages	Notification | Pager	Pager Notification

For more information about notification, refer to Chapter 5, “Notification and Reporting.”

The Security Property Page

The Security property page reflects the configuration choices made in the Security Menu.



Monitored Files: *.exe

Excluded Files: SYS:*.doc

Monitored Users: CLEVE

Directories Monitored For All Users: SYS:\login

Temporarily Authorized Users:

Figure 3-4: Security property page

The table below lists the fields displayed in the Security property page, the associated menu commands and the resulting dialog boxes.

Field	Menu Command	Dialog Box
Monitored Files	Security | Select From Master List	Select From Master List
Excluded Files	Security | Exclude Files	Exclude From Monitoring
Monitored Users	Security | Monitored Users	Monitored Users
Directories Monitored For All Users	Security | Monitor for All Users	Monitor for All Users
Temporarily Authorized Users	Security | Temporary Authorization	Temporary Authorization

For more information about security, refer to Chapter 6, “Security.”

Attaching File Servers

You must establish communication between the NetShield application console and a file server running NetShield. Attaching to a file server does not log you in as a user to that file server.

NOTE: NETSHLD.NLM must be loaded on the desired file server(s). Refer to “Loading NLMs” in Chapter 2, “Installation,” for more information.

Attaching to File Servers

To attach to a file server:

1. Choose File | Open, or click on the Select Server button from the Tool bar.

   The NetShield Servers dialog box is displayed with a listing of file servers with NETSHLD.NLM loaded.

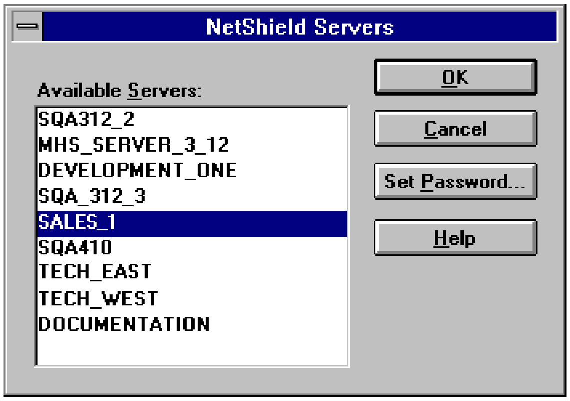


Figure 3-5: Selecting servers

2. Select the desired file server from the list provided.
3. Choose OK.

   The NetShield Password dialog box is displayed.

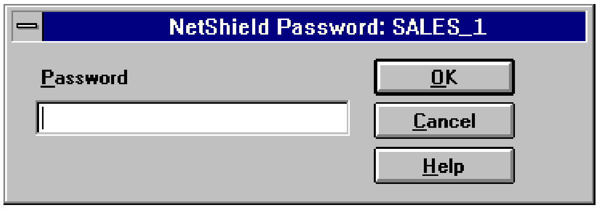


Figure 3-6: The NetShield Password dialog box

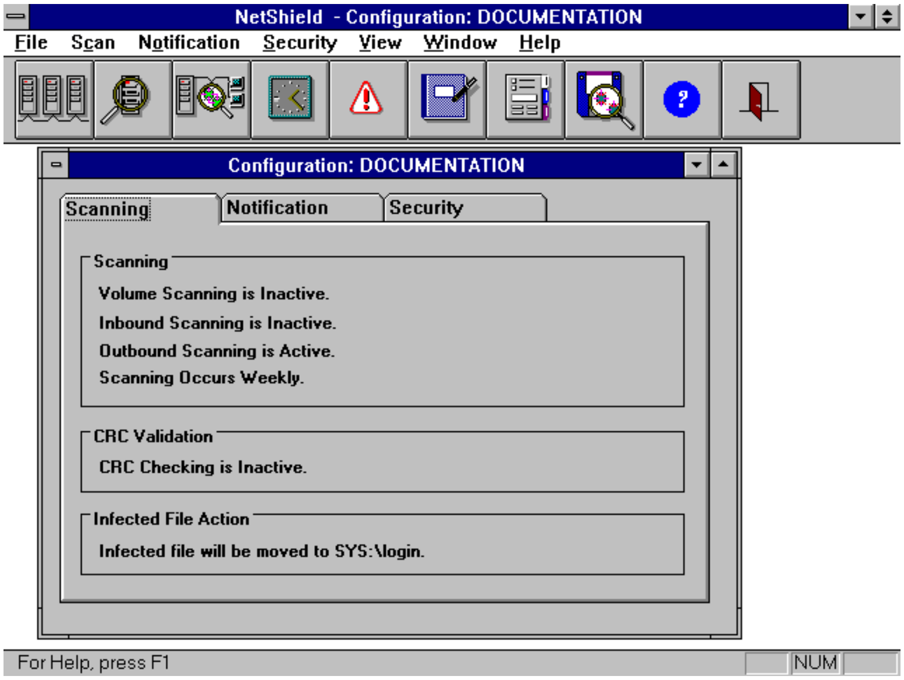
4. Enter your NetShield password in the provided text box.

   NOTE: This process only attaches you to the selected file server to allow communication between the NetShield application console and the file server running NETSHLD.NLM. You are not logged in as a user.

   You can change a file server’s password by selecting the file server and choosing Set Password. For more information, refer to “Changing Your Password” later in this chapter.

5. Choose OK.

   The NetShield console is displayed with the selected file server in the configuration window.


NetShield - Configuration: DOCUMENTATION
File Scan Notification Security View Window Help
Configuration: DOCUMENTATION
Scanning
Notification
Security
For Help, press F1
NUM

Scanning

Volume Scanning is Inactive.

Inbound Scanning is Inactive.

Outbound Scanning is Active.

Scanning Occurs Weekly.

CRC Validation

CRC Checking is Inactive.

Infected File Action

Infected file will be moved to SYS:\login.

Figure 3-7: The NetShield console displaying the NetShield Configuration for file server Documentation

Changing Your Password

You can set a unique NetShield password for each file server. Use the following procedure to set your NetShield password.

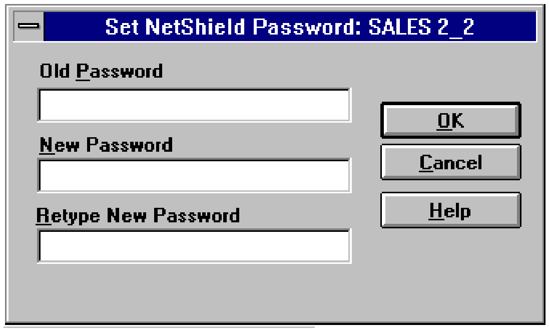
NOTE: Your NetShield password is used for attaching to file servers. The default for this password is `NETSHIELD.` Your security password is used for enabling the security menu. The default for this password is `LOGIN ADMIN.` For more information about your security password, see Chapter 6, “Security.”

1. Choose File | Open, or click on the Open button from the Tool bar.

   The NetShield Servers dialog box is displayed.

2. Select the file server you want to change the password for, and choose Set Password.

   The Set Password dialog box is displayed.


Set NetShield Password: SALES 2_2

Old Password

New Password

Retype New Password

Figure 3-8: Setting the NetShield password for file server SALES 2_2

3. Enter the old and new passwords in the provided fields, then retype the new password in the provided field.
4. Choose OK.

   NetShield saves the new password and attaches you to the selected file server.

Exiting NetShield

Use the following procedure to end a NetShield windows session.

NOTE: The following procedure does not unload the NETSHLD.NLM from any file servers. For further information, refer to “Loading NLMs” in Chapter 2, “Installing NetShield.”

1. Choose File | Exit, or click on the Exit button from the Tool bar.

   The NetShield console closes and returns you to your Windows desktop.

Detaching from File Servers

To detach from a file server:

1. Choose File | Close.

   The NetShield Servers dialog box for the current server is closed.

   NOTE: This procedure does not unload NETSHLD.NLM from any file servers. For further information, refer to “Loading NLMs” in Chapter 2, “Installing NetShield.”

Configuration Files

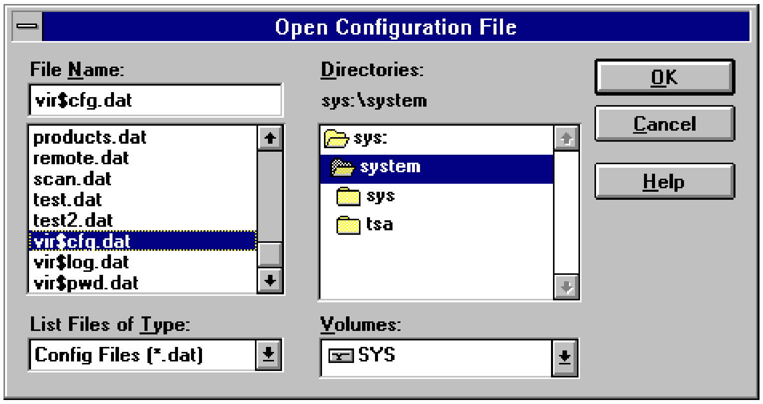
After you have configured NetShield's scanning, notification, and security options to meet your network's specific needs, you can save the configuration as a NetShield configuration file so you can quickly apply this configuration to other file servers in your enterprise.

Loading Configuration Files

NetShield should be configured to your network's virus security needs and the settings saved in a configuration file so they can be quickly applied to the other file servers on your network. To load a configuration file, perform the following procedure:

1. Choose File | Load Configuration.

   The Open Configuration File dialog box will be displayed.



File Name: vir$cfg.dat

Directories: sys:\system

List Files of Type: Config Files (*.dat)

Volumes: SYS

Figure 3-9: Managing configuration files

2. Select the desired configuration file.

   Choose a path from the Directories window.

   Enter the filename in the File Name field.

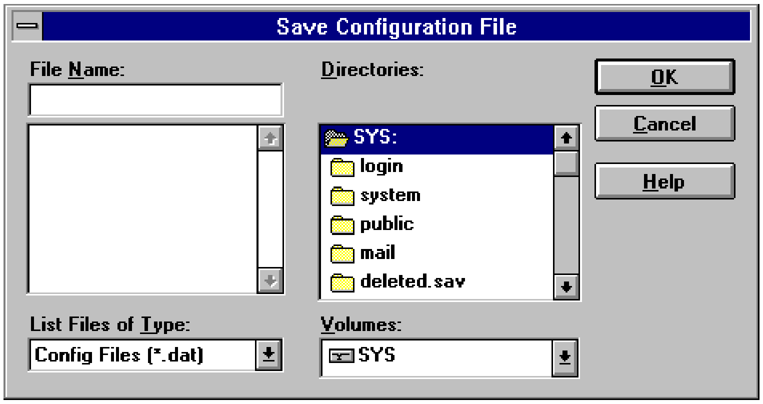
3. Choose OK to load the configuration file and return to the NetShield console. Note the changes that have been applied to the Scanning, Notification, and Security property pages.

Saving Configuration Files

NetShield’s scanning, notification and security settings can be saved to a configuration file. This configuration can then be quickly applied to other file servers in your network by attaching to the file server and loading the configuration file. To save a configuration file:

1. Choose File | Save Configuration, or click on the View Configuration button from the tool bar.

   The Save Configuration File dialog box will be displayed.



List Files of Type: Config Files (*.dat)

Volumes: SYS

Figure 3-10: Managing configuration files

2. Enter a filename (with the .dat extension) and path for the configuration file.
3. Choose OK.

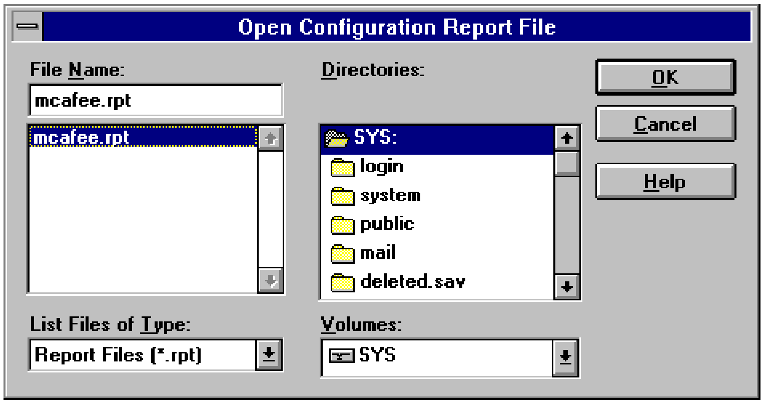
   The configuration file will be saved and you will be returned to the NetShield console.

Viewing Configuration Files

You can view or print a configuration report file (with a .RPT extension) to see how NetShield’s scanning, notification and security options are configured. The file will be displayed through Windows Write. Configuration report files are saved through the File Server Console (refer to “Configuration File Management” in Chapter 7, “The NetShield Console”). To view a previously saved configuration file:

1. Choose View | View Configuration File or click on the View Configuration button from the tool bar.

   The Open Configuration File dialog box will be displayed.



File Name: mcafee.rpt

mcafee.rpt

Directories: SYS:

List Files of Type: Report Files (*.rpt)

Volumes: SYS

Figure 3-11: Managing configuration files

2. Select the file (with a .RPT extension) you want to view.

   Choose a path from the Directories window.

   Enter a filename in the File Name field.

3. Choose Convert.

   The selected file is displayed through Windows Write.

4. Choose File | Print to print the configuration file.

5. Choose File | Exit to close Windows Write and return to the NetShield Console.

Chapter 4 Scanning

Chapter 3 provided information about the NetShield application console. This chapter introduces and discusses NetShield's scanning options.

Overview

NetShield offers several options for scanning, including on demand scanning, on access scanning and periodic scanning. You can also take advantage of virus-tracking features like CRC validation to search for new or unknown viruses.

NOTE: Before performing a scan, be sure to configure NetShield's infected file action in case infected files are detected.

Scanning Options

NetShield offers several methods for protecting your network from viral infection and proliferation. Depending on your network's environment and your user's habits, you may require some or all of the following features to protect your network:

- **On Demand Scanning,** allowing you to perform an immediate scan of selected volumes from the attached server.
- **On Access Scanning,** for automatic scanning for infected files before they are copied to and/or from network servers.
- **Periodic Scanning,** for scheduled scans of servers on a daily, weekly, or monthly basis.

  NOTE: Configure NetShield's Infected File Action before scheduling any scans should NetShield detect an infected file. Refer to “Infected File Actions” later in this chapter.

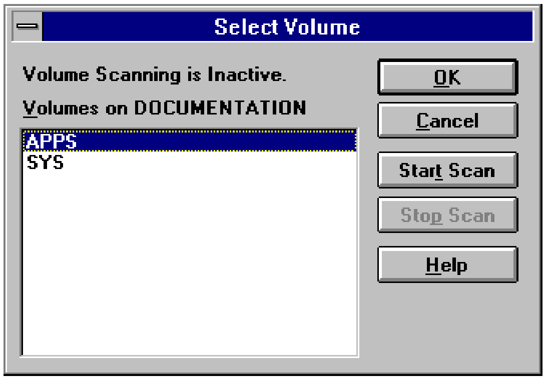
On Demand Scanning

You can schedule an immediate scan of one or more volumes on the current server. (To attach to a server, refer to “Attaching Servers” in Chapter 3, “The NetShield Console.”)

To schedule an immediate scan:

1. Choose Scan | Volume, or click on the Scan Server Now button from the tool bar.

   The Select Volume dialog box is displayed.



Volume Scanning is Inactive.

Volumes on DOCUMENTATION

APPS
SYS

Figure 4-1: Selecting Volumes to scan

2. Select one or more volumes to scan in the provided list box.

NOTE: The current server is displayed in the Volumes on <Volume Name> field. All volumes for the current server are listed in the provided list box regardless of your network mappings. To select another server, refer to “Attaching Servers” in Chapter 3, “The NetShield Console.”

3. Choose Start Scan.

   The Volume Scanning field will update to Currently Scanning Volume <Volume Name>. In addition, the Currently Scanning Volume <Volume Name> field is updated in the Scanning property page in the NetShield Configuration window. For further information regarding the Scanning property page, refer to Chapter 3, “The NetShield Console.”

4. Choose Stop Scan to halt a scan in progress.

NOTE: Choosing Cancel will not stop a scan in progress. To stop the scanning process, choose Stop Scan. This will halt, not pause, the scanning process; the next time Start Scan is chosen, NetShield will restart the scan again from the beginning.

5. Choose OK to return to the NetShield console.

On Access Scanning

On Access Scanning allows NetShield to scan whenever specified files are written to and/or from a protected file server. Inbound Scanning protects your server from infection; Outbound Scanning prevents infection of a workstation. for example, if a user copies an infected file to the server, Inbound Scanning will alert any users (see Chapter 5, “Notification and Reporting”) and take whatever action has been specified (see “Infected Action” later in this chapter).

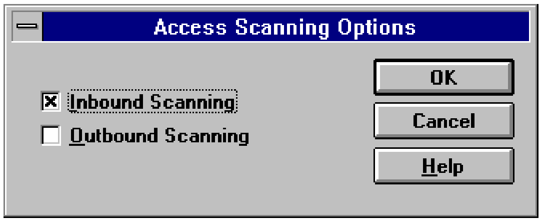
NOTE: The Outbound Scanning option does not protect the server volume against infected files copied to it, and is recommended only in cases where the server volume is read-only and might contain infected files.

On Access Scanning can be limited to a Currently Scanned Extensions List is displayed. NetShield is pre-configured to scan for executable file extensions (.BIN, .COM, .DLL, .EXE, .OVL and .SYS). You can disable this feature to have NetShield scan all files written to and/or from the server. This list can be edited through the File Server Console. Refer to “Configuring the Scanning Mode” in Chapter 7, “The File Server Console.”

To configure On Access Scanning:

1. Choose Scan | On Access.

   The Access Scanning Options dialog box is displayed.



☒ Inbound Scanning
□ Outbound Scanning

Figure 4-2: Selecting Access scanning options

2. Select the corresponding check box for the desired scanning option(s).

- **Inbound Scanning**

  Selecting this option prevents the writing of infected files to the selected server volume. During a write operation, NetShield checks the file on the target volume and, if infected, performs the specified infected file and notification actions. For further information, refer to “Infected File Action” later in this chapter and Chapter 5, “Notification and Reporting.”

- **Outbound Scanning**

Selecting this option prevents the writing of infected files from selected server volumes to other server or workstation volumes. During a write operation, NetShield checks the file on the source volume and (if infected) performs the specified infected file and notification actions. For further information, refer to “Infected File Actions” later in this chapter and Chapter 5, “Notification and Reporting.”

3. Choose OK to return to the NetShield console.

   The Inbound and Outbound fields in the Scanning property page are updated to reflect the changes made in the Access Scanning Options dialog box. For further information regarding the Scanning property page, refer to Chapter 3, “The NetShield Console.”

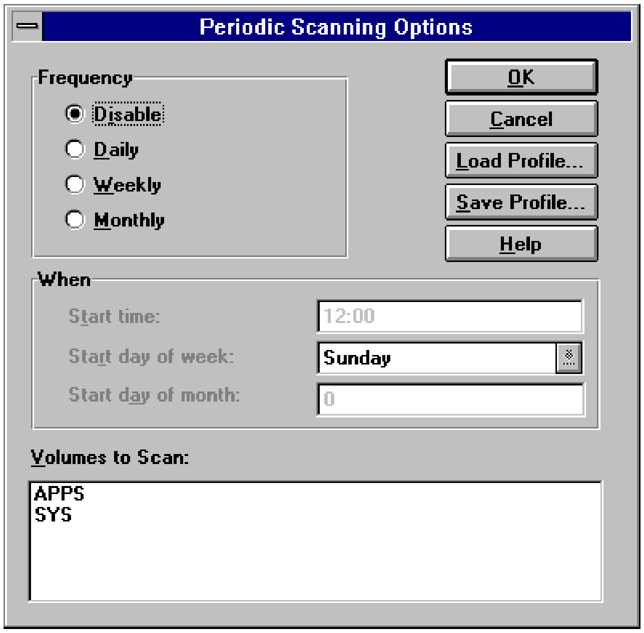
Periodic Scanning

Scanning can be scheduled on a daily, weekly, or monthly basis. For the best network performance, schedule scanning during periods of low network traffic and before system backups.

To schedule Periodic Scanning:

1. Choose Scan | Periodic.

   The Periodic Scanning Options dialog box is displayed.



Frequency

● Disable
○ Daily
○ Weekly
○ Monthly

When

Start time: 12:00

Start day of week: Sunday

Start day of month: 0

Volumes to Scan:

APPS
SYS

Figure 4-3: Selecting Periodic Scanning Options

2. Select the corresponding radio button to specify when scanning should occur.

   When chosen, several of the radio buttons enable associated fields in the When group box. Enter values in the associated fields to specify when scanning should occur. The following table lists the radio buttons, fields and values.

Radio Button	Field	Value
Disable	None	None
Daily	Start time	Enter the time of day you want the scan to begin (00:01 to 24:00)
Weekly	Start time	Enter the time of day you want the scan to begin (00:01 to 24:00)
	Start day of week	Enter the day of the week you want the scan to begin (Sunday to Saturday)
Monthly	Start time	Enter the time of day you want the scan to begin (00:01 to 24:00)
	Start day of month	Enter the day of the month you want the scan to begin (1-31)

3. Select the desired volumes to scan in the provided list box.
4. To save the selected scanning configuration, choose Save Profile.
5. To load a previously saved scanning configuration, choose Load Profile.
6. Choose OK to return to the NetShield console.

   The Periodic Scanning field located in the Scanning property page is updated to reflect changes made in the above procedure. For further information regarding the Scanning property page, refer to Chapter 3, “The NetShield Console.”

Cyclic Redundancy Check Validation

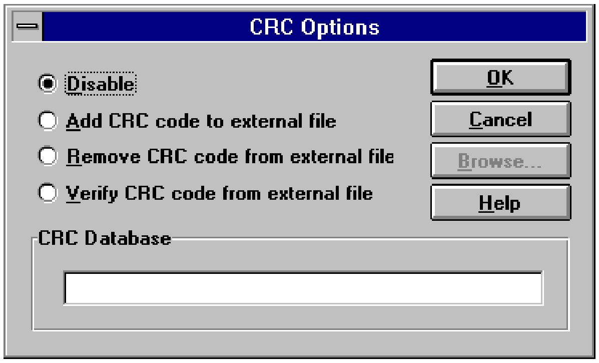
Cyclic Redundancy Check (CRC) validation is a method for discovering unknown or new viruses. NetShield calculates a number based on the nature and size of the file, then, when CRC verification is enabled, periodically recalculates that number and compares it to the original number. If the CRC has changed, it is likely that the file is infected by an unknown virus. Because the CRC code will change whenever a file is updated, it is recommended that CRC validation only be used in stable environments where few software updates are performed. Also, it is recommended that you do not perform CRC validation on data files, batch files, bindery files, or other files that are changed frequently.

Setting CRC Options

To configure Cyclic Redundancy Check Validation:

1. Choose Scan | CRC Options.

   The CRC Options dialog box is displayed.



CRC Options

● Disable
○ Add CRC code to external file
○ Remove CRC code from external file
○ Verify CRC code from external file

CRC Database

Figure 4-4: Setting CRC Options

2. Select the corresponding radio button for the desired option:

   - **Disable**

     Select this option to disable the CRC options. This is the recommended setting for most networks.

   - **Add CRC code to external file**

     Selecting this option prompts NetShield to add CRC validation codes to the external database file during the next scan. Any previous validation codes must be removed from the selected database file before proceeding. This option should be disabled once the validation codes have been added and should not be selected again until the validation codes are deleted using the Remove radio button (described below).

   - **Remove CRC code from external file**

     Once you have added CRC validation codes to the database, selecting this option prompts NetShield to remove the validation codes during the next scan from the selected database file. You normally do this if you have added or upgraded software on your network and need to update the validation codes.

- **Verifying CRC code from external file**

  Once you have added CRC validation codes to the database, selecting this option prompts NetShield to check for validation codes in subsequent scans and, if the files have changed, to warn that infection by an unknown virus may have occurred.

3. Enter the CRC database name in the provided text box choose OK.

   By default, the database file used to store CRC validation codes is named VIR$CRC.DAT which is stored in the same directory as the NETSHLD.NLM file. The name and location of the database file can be changed as needed.

   The CRC Validation group box located in the Scanning property page is updated to reflect changes made in the above procedure. For further information regarding the Scanning property page, refer to Chapter 3, “The NetShield Console.”

Infected File Actions

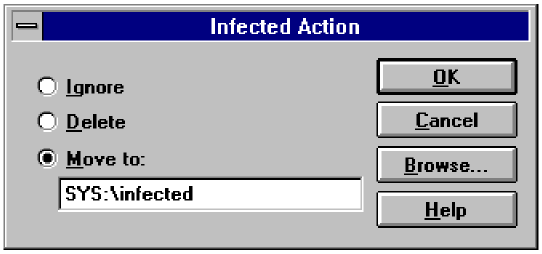
NetShield allows you to predefine what action should be taken if infected files are detected. Infected files can be deleted, ignored, or moved to a “quarantine” directory. McAfee recommends moving the files so that they can be examined later. Most infected files can be cleaned using McAfee’s desktop anti-virus solution, VirusScan, or can even be uploaded to McAfee for expert inspection by McAfee’s team of virus researchers. For more information, refer to “McAfee Support” in Chapter 1, “Introducing NetShield.”

Setting Infected Action Options

To configure Infected File Action:

1. Choose Scan | Infected Action.

   The Infected Action dialog box is displayed.



○ Ignore
○ Delete
● Move to:
SYS:\infected

Figure 4-5: Determining detection action

2. Select the corresponding radio button for the desired option.

- **Ignore Infected Files**

  Select this option to ignore infected files found during a scan. NetShield leaves any infected files intact on your system, which could result in the transmission of the virus to other nodes on the network. However, all virus identification is recorded in the NetShield activity log if Logging (see Chapter 5, “Notification and Reporting”) is enabled. If you choose to use this setting, we recommend that you check the log files for infected files immediately after scanning and, if found, take steps to protect your system.

  WARNING: This option is less secure than other options. Infected files might still be copied to the server and *viruses might spread even when NetShield is active.*

- **Delete Infected Files**

  Select this option to delete infected files found during a scan. NetShield erases any infected files and writes random characters to the disk space formerly occupied by the infected file. As a result, this file is completely eradicated from your network and is not recoverable except from backups. This is the most secure option, but it can prevent you from recovering an infected file you might want to save for further inspection.

  NOTE: Be sure to enable Logging (refer to Chapter 5, “Notification and Reporting”) or you will not know which files NetShield has deleted.

- **Move Infected Files**

  Select this option to move infected files found during a scan. NetShield will move the infected files to a different directory so that you can inspect them yourself, possibly clean the infected files using McAfee’s desktop anti-virus solution, VirusScan, or upload them to McAfee for expert inspection. To avoid a situation where users could inadvertently load an infected file and spread the virus, the directory you specify should be a “quarantine directory” to which only system administrators have access. We suggest that you exclude this directory from future scanning (refer to “Excluding

Directories" later in this chapter) to avoid redundant identification and notification. Enter the path of the "quarantine directory" in the field provided or choose Browse to search for a path.

4. Choose OK to return to the NetShield console.

   The Infected Action group box located in the Scanning property page. For further information regarding the Scanning property page, refer to Chapter 3, "The NetShield Configuration Window."

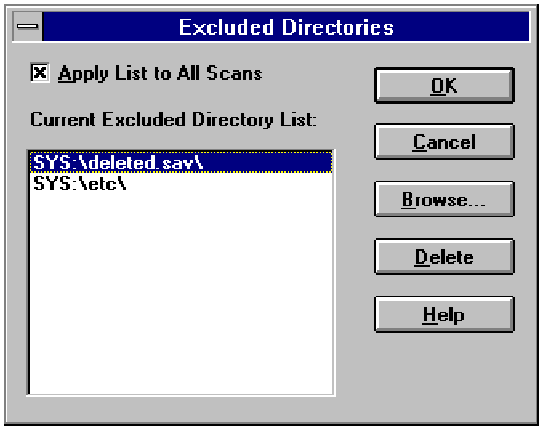
Excluding Directories

You may want to exclude specific directories from scans to reduce scanning time. For example, you may want to exclude read-only directories from scans if you are confident that they are not at risk for viral infection. We recommend that you exclude "quarantine" directories from scans to avoid redundant identification and notification (refer to "Infected File Actions" earlier in this chapter).

To exclude a directory from scanning:

1. Choose Scan | Exclude Directories.

   The Excluded Directories dialog box is displayed.



Excluded Directories

☒ Apply List to All Scans

Current Excluded Directory List:

SYS:\deleted.sav\
SYS:\etc\

Figure 4-6: Excluding directories from a scanning event

2. To apply the current list of excluded directories from all scanning events, select the Apply List to All Scans check box.

   NOTE: Listed directories will not be excluded from scans unless this check box is selected.

3. Choose Browse to add to the excluded directory list.

The Select Directory dialog box is displayed.

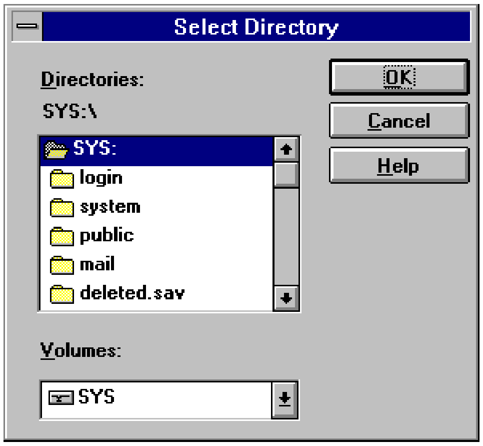


Figure 4-7: Selecting directories to be excluded

4. After selecting the desired directory to exclude, choose OK.

   Repeat Steps 3 and 4 for each directory you want to exclude.

5. To remove a directory from the exclusion list, select the directory and choose Delete.

6. Choose OK to save and return to the NetShield console.

Cross Server Updating

NetShield's SCAN.DAT and NAMES.DAT files are regularly updated to detect new viruses and variants of old ones. When you download updates of NetShield data files from McAfee, you can use NetShield's cross server updating feature to automatically upgrade NetShield data files everywhere NetShield is installed on your network. Cross server updating saves you the effort of performing this task manually for each server.

For cross server updating to work for all NetShield servers on your network, you must enable it for each NetShield installation. Once enabled, NetShield periodically sends a message to other servers, via NetWare's Service Advertising Protocol (SAP), which requests each server to indicate its version of the data files. NetShield retrieves these messages from other servers and, if another NetShield installation has a more recent version of the data files, obtains these files immediately from the other installation. In this way, you can update the data files on one server and have them propagate automatically to all servers.

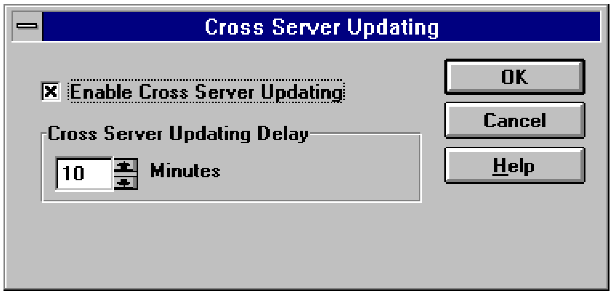
For more information on updating NetShield data files from McAfee, refer to “McAfee Support” in Chapter 1, “Introducing NetShield.”

Using Cross Server Updating

To enable Cross Server Updating:

1. Choose Scan | Cross Server Updating.

   The Cross Server Updating dialog box is displayed.



Cross Server Updating

☒ Enable Cross Server Updating

Cross Server Updating Delay

10 Minutes

Figure 4-8: Enabling Cross Server Updating

2. To enable cross server updating, select the corresponding check box.

   The Cross Server Updating Delay group box is enabled.

3. You can schedule the frequence of NetWare SAP messages from once every minute to once every 25 minutes. The default setting is once every ten minutes.

   Use the spin controls to enter a value (in minutes) between 1 and 25.

4. Choose OK to return to the NetShield console.

If You Detect a Virus

McAfee strongly recommends that you obtain experienced help in dealing with viruses if you are unfamiliar with anti-virus software and methods. This is especially true for “critical” viruses, because improper removal of these viruses can result in the loss of all data and the use of infected disks.

If you are at all unsure about how to proceed once you have found a virus, contact McAfee for assistance. Refer to “McAfee Support” in Chapter 1.

Chapter 5 Notification and Reporting

Chapter 4 provided information about the NetShield scanning options. This chapter introduces and discusses NetShield’s notification and reporting options.

Overview

NetShield offers several options for notification upon virus detection, including network broadcasts, console messages, e-mail notification, and pager notification. NetShield can also keep a record of scanning events and results in a log file.

Logging

Logging is an important tool in network security because it can provide clues about the source and spread of viral infection, as well as providing a means for measuring viral activity. NetShield has a logging option so you can have a record of scanning events and results.

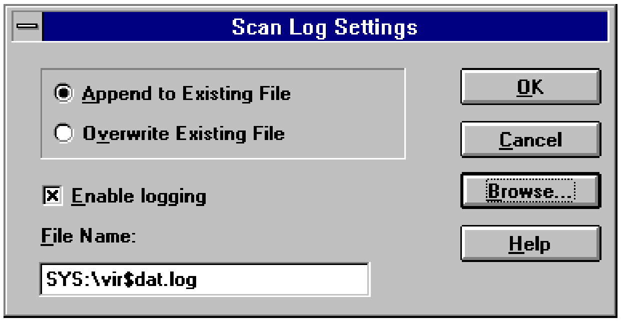
Selecting Scan Log Settings

McAfee recommends that you enable logging whenever you scan so that you have an audit trail of infections found and infected file actions.

To enable logging:

1. Choose Notification | Logging.

   The Scan Log Settings dialog box is displayed.



Scan Log Settings

● Append to Existing File

○ Overwrite Existing File

☒ Enable logging

File Name: SYS:\vir$dat.log

Figure 5-1: Scan log settings

2. Select the Enable Logging check box.
3. Enter a file name in the provided text box or choose Browse to locate the desired file and choose OK.
4. Choose Append to Existing File to have NetShield attach the scan results to the end of an existing scan log file. Choose Overwrite Existing File to delete the old scan log file and save the new log file in its place.

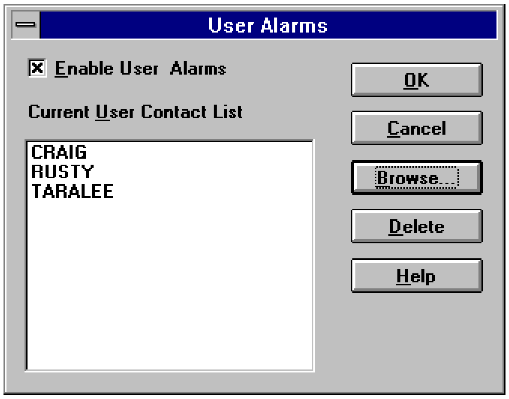
Enabling User Notification

NetShield can alert selected users that infected files have been detected during a scan with a network broadcast message.

To enable user notification:

1. Choose Notification | User.

   The User Alarms dialog box is displayed.



User Alarms

☒ Enable User Alarms

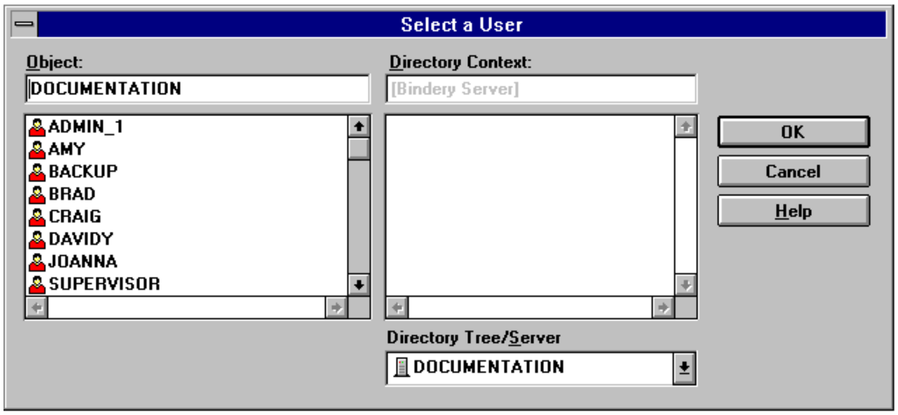
Current User Contact List

CRAIG
RUSTY
TARALEE

Figure 5-2: User Alarms dialog box

2. Select the Enable User Alarms check box.
3. Choose Browse to add a user to the Current User Contact list.

   The Select a User dialog box is displayed.



Select a User

Object: DOCUMENTATION

Directory Context: [Bindery Server]

ADMIN_1
AMY
BACKUP
BRAD
CRAIG
DAVIDY
JOANNA
SUPERVISOR

Directory Tree/Server: DOCUMENTATION

Figure 5-3: Select a User dialog box

NOTE: The directory tree will not be displayed unless you are logged in as a NetWare Directory Services (NDS) user.

4. Select an attached file server or directory tree from the drop-down list provided.
5. Select one or more users from the Objects provided.
6. Choose OK to return to the User Alarms dialog box.

   The selected user(s) are now displayed in the Current User Contact List.
7. To remove one or more users from the Current User Contact List, select the user(s) and choose Delete.

   The selected user(s) are now removed from the Current User Contact List.
8. Choose OK to return to the NetShield console.

   The Notification property page is updated to reflect the changes you have made.

Enabling Mail Notification

NetShield can use e-mail to alert selected users that infected files have been detected. NetShield delivers the alert messages through Novell’s Global Message Handling Service (GMHS), which can route e-mail messages throughout your network or through mail gateways to external mail services.

NOTE: To use this feature, you must have Novell Basic or Global MHS installed and running on your network.

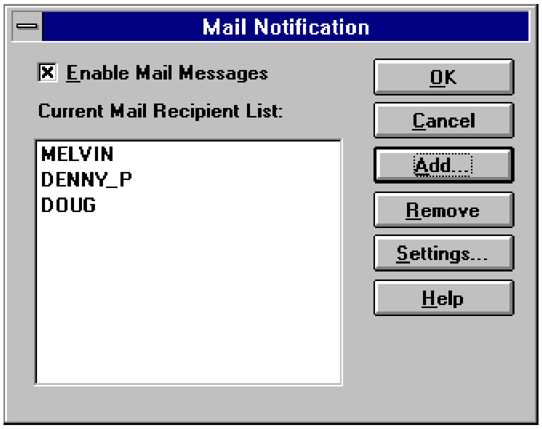
If NetShield detects a virus during volume scanning, NetShield sends mail notifications once to the selected users after scanning is concluded. If On Access Scanning is enabled (refer to “Selecting Access Scanning Options” in Chapter 3, “Scanning”), however, NetShield sends a notification as soon as a virus is detected. This could lead to a backlog of redundant notifications if many infected files are detected. If, for example, a user attempts to copy 20 infected files to a monitored server, NetShield will send 20 notifications to each of the selected users.

To prevent such a backlog, you can set a Minimum Message Interval, in minutes, that NetShield should wait before sending a new notification. Using the above example, if the Minimum Message Interval is set to 5 and all 20 infected files are copied within five minutes, NetShield sends only one message. If it takes 16 minutes to copy all 20 infected files, NetShield sends three messages.

To enable mail notification:

1. Choose Notification | Mail.

   The Mail Notification dialog box is displayed.



Mail Notification

☒ Enable Mail Messages

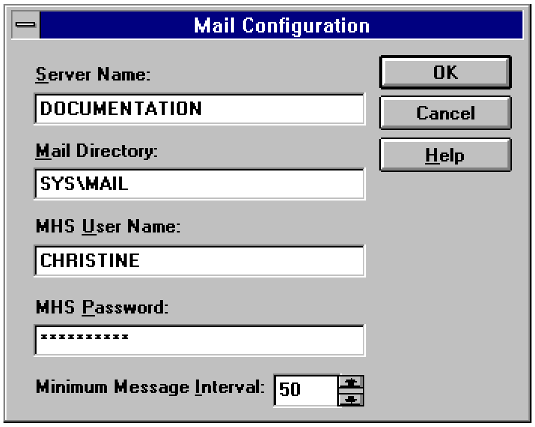
Current Mail Recipient List:

MELVIN
DENNY_P
DOUG

Figure 5-4: Mail Notification

2. Select the Enable Mail Messages check box.
3. Choose Settings to configure NetShield to your Novell Basic or Global MHS setup.

   The Mail Configuration dialog box is displayed.



Server Name: DOCUMENTATION

Mail Directory: SYS\MAIL

MHS User Name: CHRISTINE

MHS Password: **********

Minimum Message Interval: 50

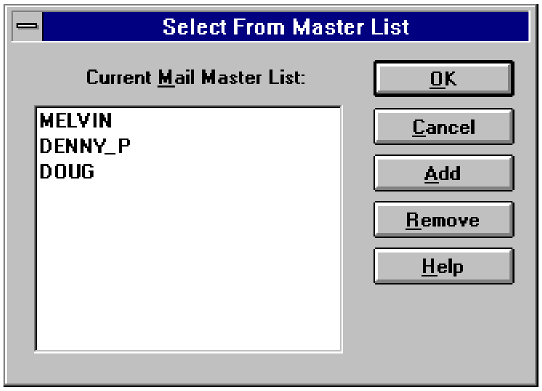
Figure 5-5: Mail Configuration

Enter the following information in the corresponding fields:

- **Server Name,** which is the name of the server running GMHS;
- **Mail Directory,** the directory GMHS is installed in on the server;
- **MHS User Name,** the user name NetShield uses when attaching to the GMHS server;
- **MHS Password,** the password for the user name used above; and
- **Minimum Message Interval,** for NetShield to use when it is not specified for an active user.

4. Choose OK to return to the Mail Notification dialog box.
5. Choose Add to add a user to the Current Mail Recipient list.

   The Select From Master List dialog box is displayed.



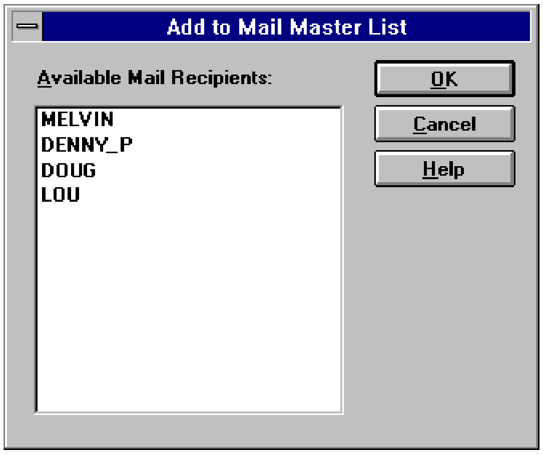
Current Mail Master List:

MELVIN
DENNY_P
DOUG

Figure 5-6: Selecting from Mail Master List.

6. Select a user from the Current Mail Master List.
7. To add a user from the selected server to the Current Mail Master List, choose Add.

   The Add to Mail Master List dialog box is displayed.



MELVIN
DENNY_P
DOUG
LOU

Figure 5-7: Adding to the Mail Master List.

8. Select a user from the Available Mail Recipients list and choose OK to add the user to the Current Mail Master List and return to the Select From Master List dialog box.

NOTE: If the desired user is not listed in the Available Mail Recipients list, your GMHS settings may be configured incorrectly. Choose Cancel to return to the Select From Master List dialog box, then choose Cancel again to return to the Mail Notification dialog box. Choose Settings and ensure your GMHS is correctly configured.

9. Choose OK to return to the Mail Notification dialog box.

   The selected user is now displayed in the Current Mail Recipient List.
10. To delete a user from the Current Mail Recipient List, select the user and choose Remove.

    The selected user is now removed from the Current Mail Recipient List.
11. Choose OK to return to the NetShield console.

Enabling Pager Notification

NetShield can page selected users if infected files have been detected. NetShield dials standard pager numbers and sends your message to selected network administrators and support personnel.

NOTE: To use this feature, you must have a Hayes-compatible modem installed, running, and accessible on your NetShield server.

If NetShield detects a virus during volume scanning, NetShield sends pager notifications once to the selected users after scanning is concluded. If on access scanning is enabled (refer to “Selecting Access Scanning Options” in Chapter 3, “Scanning”), however, NetShield sends a notification as soon as a virus is detected. This could lead to a backlog of redundant pager notifications if many infected files are detected. If, for example, a user attempts to copy 20 infected files to a monitored server, NetShield will send 20 notifications to each of the selected users.

To prevent such a backlog, you can set a Minimum Message Interval, in minutes, that NetShield should wait before sending a new notification. Using the above example, if the Minimum Message Interval is set to 5 and all 20 infected files are copied within five minutes, NetShield sends only one message. If it takes 16 minutes to copy all 20 infected files, NetShield sends three messages.

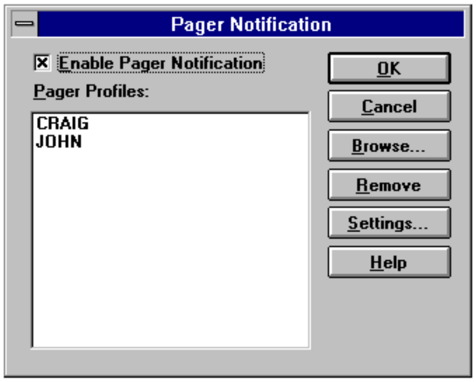
SFT III NOTE: SFT III does not support pager notification.

NETWARE NOTE: AIOCOMX.NLM and AIO.NLM must be loaded in order to use pager notification on a Novell NetWare 3.X or 4.X server.

To enable pager notification:

1. Choose Notification | Pager.

   The Pager Notification dialog box is displayed.



Pager Notification

☒ Enable Pager Notification

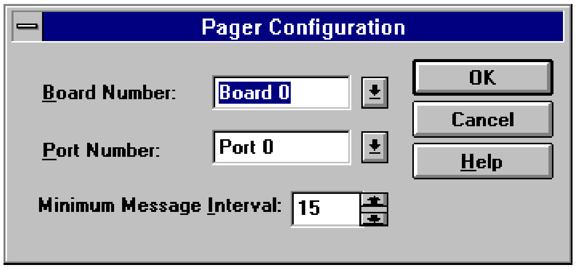
Pager Profiles:

CRAIG
JOHN

Figure 5-5: Pager Notification

2. Select the Enable Pager Notification check box.
3. Choose Settings to configure NetShield to your modem setup.

   The Pager Configuration dialog box is displayed.



Board Number: Board 0

Port Number: Port 0

Minimum Message Interval: 15

Figure 5-6: Pager Configuration

Enter the following information in the corresponding fields:

- **Board Number,** as defined by the AIOCOMX.NLM utility, which determines the board number of the modem installed on your NetShield server;
- **Port Number,** as defined by the AIOCOMX.NLM utility, which determines the port number of the modem installed on your NetShield server; and
- **Minimum Message Interval,** for NetShield to use when it is not specified for an active user.

4. Choose OK to return to the Pager Notification dialog box.
5. Choose Browse to add a user to the Select Pager Profiles list.

   The Pager Master List dialog box is displayed.

6. Select a user from the master list, or choose New to add a user to the master list.
7. Choose OK to return to the Pager Notification dialog box.

   The selected user is now displayed in the Select Pager Profiles list.

8. To delete a user from the Select Pager Profiles list, select the user and choose Remove.

   The selected user is now removed from the Select Pager Profiles list.

9. Choose OK to return to the NetShield console.

Enabling Console Messages

NetShield can alert network administrators that infected files have been detected during a scan with a message that appears on the NetWare File Server Console.

To enable console messages:

1. Choose Notification | Console Messages.

   A check mark is displayed next to Console Messages, indicating that the Console Messages command is enabled.

To disable console messages:

1. Choose Notification | Console Messages.

   The check mark next to Console Messages is removed, indicating that the Console Messages command is disabled.

For more information about the NetShield File Server Console, refer to Chapter 7, “The File Server Console.”

Chapter 6 Security

Chapter 5 provided information about the NetShield notification and reporting options. This chapter introduces and discusses NetShield's security options.

Overview

NetShield offers several options for networks requiring even tighter security. NetShield can restrict write access to specific files, directories or users. In addition, you can exclude specific files or file types from scans and you can grant temporary authorization to specific users to allow software installations or upgrades.

NOTE: Your NetLock security configuration will not be enforced if you do not select the Enable NetLock Security check box in the Security Settings dialog box.

Enabling NetShield Security

NetShield security is password-protected to ensure that only authorized users have access. This eliminates the possibility of server security changes traditionally incurred on servers managed by multiple administrators. The default password is:

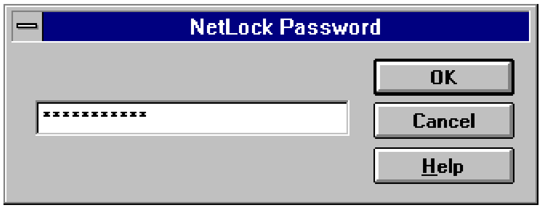
```
login admin
```

You should change this password when you run NetShield for the first time. For instructions, refer to "Edit Network Security Configuration" in Chapter 7, "The File Server Console."

To enable NetShield security:

1. Choose Security | Security Password.

   The NetLock Password dialog box is displayed.



****

Figure 6-1: Enabling NetShield Security

2. Enter the password in the provided text box.
3. Choose OK to return to the NetShield console.

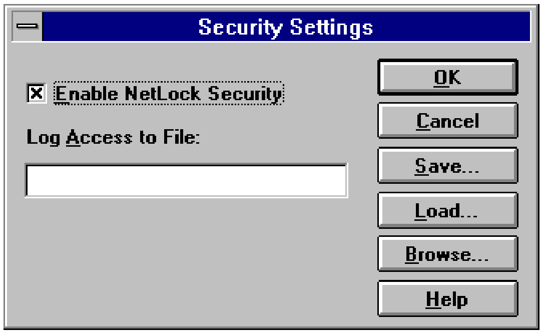
NOTE: The remainder of the Security menu is enabled once the correct password is entered.

Selecting Security Settings

The Security Settings menu allows you to enable or disable network security, create a log for unauthorized write attempts, and load or save a security configuration. To configure NetShield's security settings:

1. Choose Security | Settings.

   The Security Settings dialog box is displayed.



☒ Enable NetLock Security

Log Access to File:

Figure 6-2: Security Settings dialog box

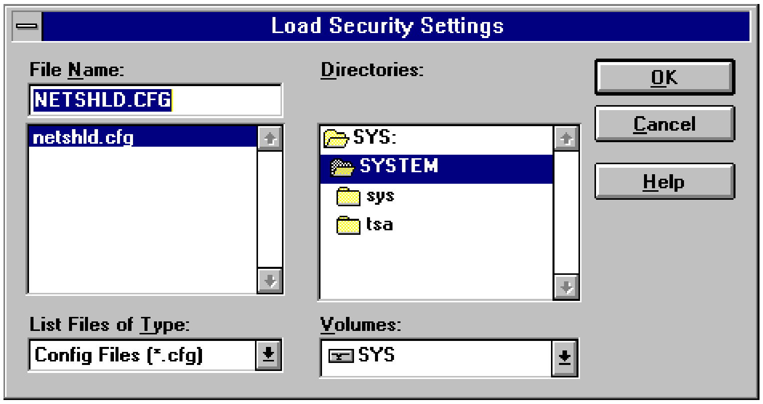
2. Select the corresponding check box to enable NetLock security.

NOTE: If NetLock security is not enabled, the security configuration will not be enforced.

3. To record unauthorized write attempts in a log file, enter a file name in the Log Access to File text box.

4. To save the security configuration options, choose Save and enter a file name.
5. To load a previously saved security configuration file, choose Load and enter a file name.
6. Choose Browse to search for a security configuration file.

   The Load Security Settings dialog box is displayed.



Load Security Settings

File Name: NETSHLD.CFG

netshld.cfg

Directories:

SYS:
SYSTEM
sys
tsa

List Files of Type: Config Files (*.cfg)

Volumes: SYS

Figure 6-3: Load Security Settings

7. Select the file you want to load and choose OK.

   The file will be loaded and you will be returned to the Security Settings dialog box.

   Choose Cancel to abort this procedure and return to the Security Settings dialog box.

Monitoring Write Access

NetShield can monitor specific files, extensions, directories, or users for write access. You can also exclude specific files or extensions from monitoring (such as backup or data files) to customize your monitoring. For example, you could restrict write access to “guest” users using the Monitored Users feature, which would deny all write access to protected volumes. You could then use the Exclude Files From Monitoring option to allow these users to save .DOC files.

NetShield can record unauthorized write attempts to a log file. Refer to “Selecting Security Settings” for more information. To view this log file, choose View | Log File or click on the View Logs tool bar button.

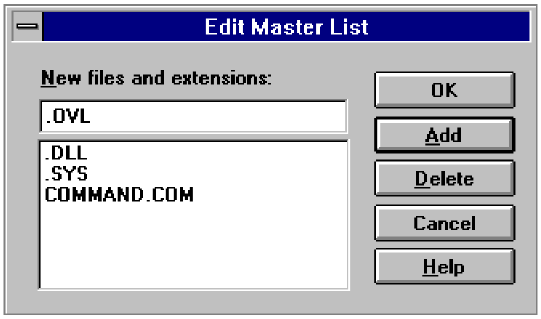
Creating a Master List of Files and File Extensions

NetShield can monitor specific files or file types for unauthorized write access. For example, you may want NetShield to monitor all executable files by adding the COM, EXE, SYS, BIN, OVL, and DLL extensions to the master list. You must first create a list of files and file extensions, then select the files or extensions you want to monitor. You will use the master list to monitor files in the next section, “Select from Master List.”

To create or edit the master list of files and file extensions:

1. Choose Security | Edit Master List.

   The Edit Master List dialog box is displayed.



Edit Master List

New files and extensions: .OVL

.DLL
.SYS
COMMAND.COM

Figure 6-4: Edit Master List dialog box

2. To add a file or extension to the list, type the name of the file or extension in the New files and extensions text box. Choose Add to add the file or extension to the master list.

   - To add an extension to the list, type a period and the extension (up to three letters).
   - To add a file to the list, type the full file name (name, period, and extension).

   NOTE: If you want NetShield to monitor these files or extensions, you must add them to another list. Refer to the next section, “Selecting from Master List.”

3. Choose OK to save and return to the NetShield console.

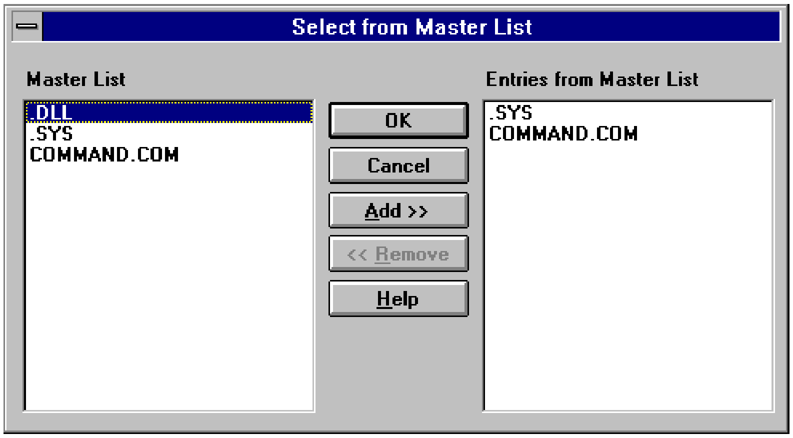
Selecting from Master List

Once you have created your master list of files and file extensions, you can select the list of entries that NetShield will monitor for unauthorized write attempts. You should monitor all standard executable file extensions (EXE, COM, SYS, BIN, OVL, and DLL). When a monitored file or extension is copied to a monitored directory, NetShield will create an entry in the log file.

To select files or extensions to monitor from the Master List:

1. Create a master list (refer to “Edit Master List,” above).
2. Choose Security | Select from Master List.

   The Select from Master List dialog box is displayed.



Select from Master List

Master List

.DLL
.SYS
COMMAND.COM

Entries from Master List

.SYS
COMMAND.COM

Figure 6-5: Select from Master List

3. Select a file or extension from the Master List window and choose Add to copy it to the Entries from Master List window.

   This file or extension will be monitored for write attempts.

4. To stop monitoring a file or extension, select it and choose Remove to delete it from the Entries from Master List window.

NOTE: Deleting a file or extension from the Entries from Master List window does not delete it from the master list. To delete a file or extension from the master list, refer to “Edit Master List,” above.

5. Choose OK to save and return to the NetShield console.

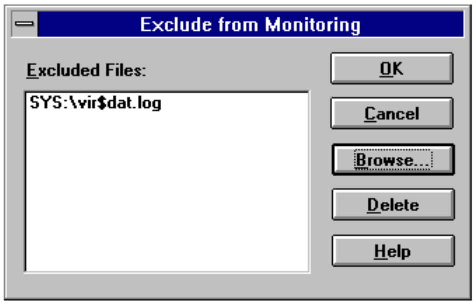
Excluding Files From Monitoring

Certain files and file extensions can be excluded from monitoring. For example, you could allow monitored users to save data files, or allow routine backups to occur in otherwise monitored directories.

To exclude files from NetLock monitoring:

1. Choose Security | Exclude Files.

   The Exclude From Monitoring dialog box is displayed.



SYS:\vir$dat.log

Figure 6-6: Excluding files from monitoring

2. Choose Browse to add to the exclusion list.

   Select the desired file and choose OK.

3. To remove a file from the exclusion list, select the desired file and choose Delete.

4. Choose OK to save and return to the NetShield console.

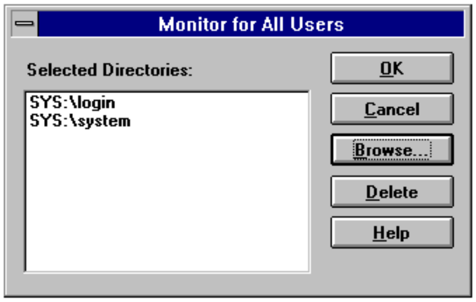
Monitor for all Users

You can protect and monitor sensitive directories for unauthorized write attempts. For example, you can monitor write access to directories that contain only application executables.

To select directories to be monitored for write attempts:

1. Choose Security | Monitor for all Users.

   The Monitor for all Users dialog box is displayed.

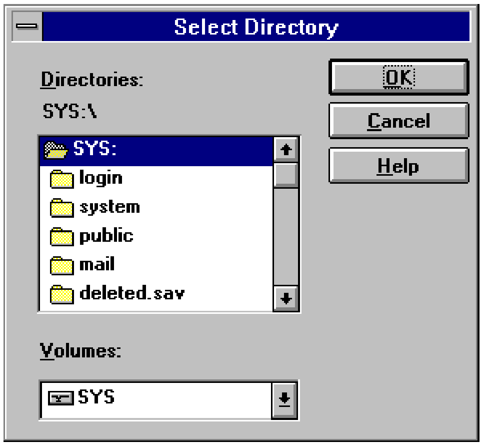


SYS:\login
SYS:\system

Figure 6-7: Selecting monitored directories

2. Choose Browse to add to the Selected Directories list.

   The Select Directory dialog box is displayed.



Directories:
SYS:\

Volumes:
SYS

Figure 6-8: Selecting monitored directories

3. Select the desired directory and choose OK.
4. To delete a directory from the Selected Directories list, select the desired directory and choose Delete.
5. Choose OK to save and return to the NetShield console.

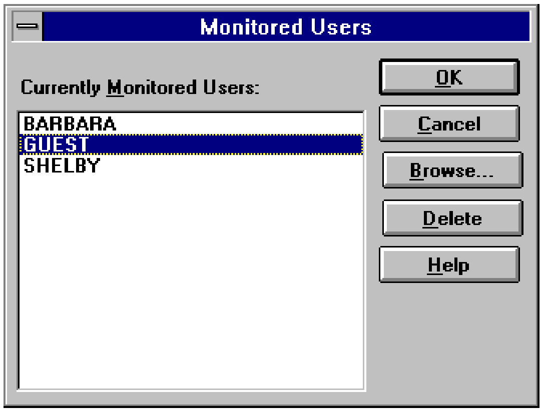
Selecting Monitored Users

You can restrict write access to specific users to prohibit write attempts to all volumes and directories. These users will have read-only access to volumes and directories protected by NetShield.

To select monitored users:

1. Choose Security | Monitored Users.

   The Monitored Users dialog box is displayed.



Currently Monitored Users:

BARBARA
GUEST
SHELBY

Figure 6-9: Selecting monitored users

2. To deny write access to a user, choose Browse to add a user to the Currently Monitored Users list.

   The user’s name is added to the Current Monitored Users list.

3. To remove a user from the Currently Monitored Users List, select the user and select Delete.

   The user’s name is removed from the Current Monitored Users list.

4. Choose OK to save and return to the NetShield console.

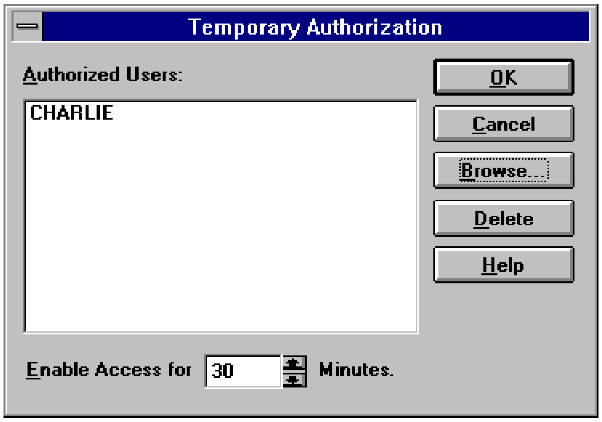
Assigning Temporary Authorization

You can suspend, for a brief time, read-only protection on monitored directories (refer to “Monitor for all Users,” above) or monitored files so that specific users can make changes. For example, you might want to allow an administrator to install or upgrade software in a monitored directory.

To assign temporary authorization:

1. Choose Security | Temporary Authorization.

   The Temporary Authorization dialog box is displayed.



Authorized Users: CHARLIE

Enable Access for 30 Minutes.

Figure 6-10: Granting temporary authorization

2. To add a user to the Authorized Users list, choose Browse.

   Locate the desired user and choose OK.

   The user's name is added to the Authorized Users list.

NOTE: Access will not be enabled if the Enable Access time is not set to at least 1 minute.

3. To remove a user from the Authorized Users list, select the user and choose Delete.

   The user's name is removed from the Authorized Users list.

4. To enable access, type a number or use the spin control to set the access time between 1 and 180 minutes, inclusive.

NOTE: If the administrative access time runs out while changes are being made to monitored directories, NetShield completes the current write operation, if any, then prevents additional changes.

5. To disable access, set the access time to 0 minutes.

6. Choose OK to save and return to the NetShield console.

Chapter 7 The File Server Console

Chapter 6 introduced and discussed NetShield's security options. This chapter contains information about the NetShield File Server Console.

Overview

Many of the scanning, notification, and security options explained in earlier chapters can be selected using the file server that is running NETSHLD.NLM. Use your keyboard to navigate through the File Server Console. Use the arrow keys to move through the menu. Use the ENTER key to make a selection. The ESCAPE key cancels the operation and returns you to the previous menu. The INSERT and DELETE keys are used to modify lists.

On Demand Scanning

To run an immediate scan from the NetShield Console:

1. Choose Immediate Scan from the NetShield Main menu.

   The Immediate Scan menu is displayed.

2. Choose Edit Volume.

   The Current Volume Selection menu is displayed.

3. Enter a selection in the provided box or press insert to browse for a volume.
4. Choose Enter.
5. Return to the Immediate Scan menu and choose Start Scan.
6. To halt a scan in progress choose Stop Scan.

For more information about on-demand scanning, refer to “On Demand Scanning” in Chapter 4, “Scanning.”

Configuring the Scanning Mode

You can configure NetShield's on access and periodic scanning options from the NetShield File Server Console.

On Access Scanning

To configure On Access Scanning from the File Server Console:

1. Choose Configure Scanning Mode from the NetShield Main menu.

   The Scanning Mode Configuration menu is displayed.

2. Choose On Access Scanning.

   The On Access Scanning menu is displayed with the following options:

   - Inbound Files Only (recommended)
   - Outbound Files Only
   - Inbound and Outbound Files
   - Disable On Access Scanning
   - Edit Scanned Extension List

3. Choose Inbound Files Only to scan for viruses whenever files are written to the file server. Choose Outbound Files Only to scan for viruses whenever files are written from the file server. Choose Inbound and Outbound Files to scan for infected files during any access. Choose Disable On Access Scanning to turn off on access scanning.

   For more information about on access scanning, refer to "On Access Scanning" in Chapter 4, "Scanning."

4. Choose Edit Scanned Extension List to specify which files NetShield should scan.

   The Included Extension Configuration menu is displayed with the following options:

   - Edit Included Extension List
   - Enable/Disable Extension Checking

5. Choose Edit Included Extension List

   The Currently Scanned Extensions list is displayed.

NOTE: NetShield is pre-configured to scan for executable file extensions (.BIN, .COM, .DLL, .EXE, .OVL and .SYS).

To add an extension to this list, press INSERT and type the extension (up to three letters, wildcards may be used). To remove an extension, highlight the extension and press DELETE.

Return to the Included Extension Configuration menu by pressing ESCAPE.

6. Enable or disable extension checking by toggling between the two choices.

NOTE: NetShield will not limit On Access Scanning to the Currently Scanned Extensions list unless extension checking is enabled.

For more information about extension checking, refer to “Configuring NetShield Scans” in Chapter 6, “Security.”

Periodic Scanning

To schedule Periodic Scanning from the File Server Console:

1. Choose Configure Scanning Mode from the NetShield Main menu.

   The Scanning Mode Configuration menu is displayed.

2. Choose Periodic Scanning to schedule automatic scanning.

   The Periodic Scanning menu is displayed with the following options:

   - Scanning
     - Enable/Disable Periodic Scanning
     - Day of Week
     - Day of Month
     - Time of Day
   - Select Volumes to Scan
   - Load Scan Settings from File
   - Save Scan Settings to File.

3. Choose Scanning to configure Periodic Scanning.

   Enable periodic scanning by hitting ENTER. The Select Scanning Frequency Menu is displayed.

   - If you choose Daily scanning, you will be prompted for the time to begin scanning. Enter the time in 24-hour format. For example, 01:00 is 1 a.m.; 13:00 is 1 p.m.

- If you choose Weekly scanning, you will be prompted for the day of the week for the scan to occur and the time to begin the scan. For example, choose Monday and 24:00 to scan every Monday at midnight.
- If you choose Monthly scanning, you will be prompted for the day of the month for the scan to occur and the time to begin the scan. For example, choose 1 and 05:00 to scan the 1st of every month at 5:00 a.m.

4. Specify which volumes to scan by choosing Select Volume to Scan.
5. Load a previously saved configuration by choosing Load Scan Settings from File.
6. Save this configuration by choosing Save Scan Settings to File.

For more information about periodic scanning, refer to “Scheduling Scans” in Chapter 4, “Scanning.”

Actions on Virus Detection

You can configure NetShield’s Infected File Action from the File Server Console. Use the settings available from the Configure Virus Detection menu to set what NetShield does with an infected file, and who should be notified upon detection of a virus.

Infected File Action

To configure Infected File Actions from the File Server Console:

1. Choose Configure Virus Detection from the NetShield Main menu.

   The Virus Detect Configuration menu is displayed with the following options:

   - Infected File Action
   - User Contact Action

2. Select Infected File Action.

   The Select Action From List menu is displayed with the following options:

   - Overwrite and Delete Infected File
   - Move Infected File
   - Ignore Infected File

3. Select the desired option.

If you choose Move Infected File the Infected File Move to Directory menu is displayed. Enter a path in the provided box or choose INSERT to locate a path.

WARNING: If you choose the “Ignore Infected File” setting, infected files might still be copied to the server and *viruses might spread even when NetShield is active*. If you are using this option, be sure to check the NetShield scan logs for infected files immediately after scanning.

You are returned to the Virus Detect Configuration menu.

For more information about Infected File Actions, refer to “Infected File Actions” in Chapter 4, “Scanning.”

User Contact Action

NetShield can alert selected users that infected files have been detected through e-mail messages, network broadcast messages, numeric pagers or file server console messages.

To configure notification options from the File Server Console:

1. Choose Configure Virus Detection from the NetShield Main menu.

   The Virus Detect Configuration Menu is displayed with the following options:

   - Infected File Action
   - User Contact Action

2. Choose User Contact Action.

   The Select User Contact Actions menu is displayed with the following options:

   - Edit MHS Configuration
   - Edit Pager Configuration
   - Edit User Contact List
   - Enable User Alarms
   - Enable Console Messages

For more information about user contact action, refer to Chapter 5, “Notification and Reporting.”

Mail Alerts

NetShield can alert selected users that infected files have been detected through Novell’s Messaging Handling Service.

To enable GMHS Alerts from the File Server Console:

1. Choose MHS Configuration from the Select User Contact Action menu.

   The Select MHS Configuration Options menu is displayed with the following options:

   - Edit Master MHS User List
   - Edit Active MHS User List
   - Edit MHS Server Configuration
   - Send Test Mail to Active List Members
   - MHS Alert Status Enabled/Disabled

2. Choose Edit Master MHS User List to add or remove users to the master list. These users will not be notified unless they are added to the Active MHS User List.
3. Choose Edit Active MHS User List to add or remove users to the active list. Adding or removing users from this list will not affect the master list.
4. Choose Edit MHS Server Configuration to setup GMHS notification.

   The Edit MHS Server Configuration menu is displayed with the following fields:

   - MHS Server Name
   - MHS Server Directory
   - MHS User Name
   - MHS User Password
   - Minimum Mail Interval

   Enter the location of GMHS (Novell’s Message Handling Service) by entering the information in the appropriate fields.

   To avoid a backlog of redundant mail messages with On Access Scanning, enter the Minimum Mail Interval time, in minutes.

5. Choose Send Test Mail to Active Members to ensure that Mail Alarms are configured correctly.
6. Enable or disable MHS Alerts by toggling between the two choices.

NOTE: NetShield will not send notification by MHS Mail unless MHS Alerts are Enabled.

For more information about MHS Alerts, refer to “Enabling Mail Messages” in Chapter 5, “Notification and Reporting.”

Pager Alerts

NetShield can alert selected users that infected files have been detected by calling their pagers if a Hayes-compatible modem is available to the NetShield file server.

To enable Pager Alerts from the File Server Console:

1. Choose Pager Configuration from the Select User Contact Action menu.

   The Select Pager Configuration Options menu is displayed with the following options:

   - Edit Master Pager List
   - Edit Active Pager List
   - Edit Pager Communication Configuration
   - Test Selected Pager(s)
   - Pager Alert Status Enabled/Disabled

2. Choose Edit Master Pager List to add or remove users to the master list. These users will not be notified unless they are added to the Active Pager List.
3. Choose Edit Active Pager List to add or remove users to the active list. Adding or removing users from this list will not affect the master list.
4. Choose Edit Pager Communication Configuration to setup GMHS notification.

   The Edit Pager Communication Configuration menu is displayed with the following fields:

   - Pager Communication Board
   - Pager Communication Port
   - Default Pager Interval

   Enter the information about your Hayes-compatible modem in the appropriate fields. The Pager Communication Board and Pager Communication Port are determined by the AIOCOMX.NLM utility.

   To avoid a backlog of redundant pager messages with On Access Scanning, enter the Pager Interval time, in minutes.

5. Choose Test Select Pager(s) to ensure that Pager Alarms are configured correctly.
6. Enable or disable Pager Alerts by toggling between the two choices.

NOTE: NetShield will not send pager notifications unless Pager Alerts are Enabled.

For more information about Pager Alerts, refer to “Enabling Pager Messages” in Chapter 5, “Notification and Reporting.”

User Alerts

NetShield can alert users that infected files have been detected through a network broadcast message.

To enable User Alarms from the File Server Console:

1. Choose Enable User Alarms from the Select User Contact Action menu.

   Press “Y” to enable User Alarms or “N” to disable User Alarms.

For more information about User Alarms, refer to “Enabling User Alarms” in Chapter 5, “Notification and Reporting.”

Console Messages

NetShield can alert network administrators that infected files have been detected with a message on the NetShield File Server Console.

To enable Console Messages from the File Server Console:

1. Choose Enable Console Messages from the Select User Contact Action menu.

   Press “Y” to enable Console Messages or “N” to disable Console Messages.

For more information about Console Messages, refer to “Enabling Console Messages” in Chapter 5, “Notification and Reporting.”

Configuring the NetShield NLM

You can configure the NetShield NLM from the NetShield File Server Console to meet the specific needs of your networking environment.

Configuration File Management

You can save, load, view, or print a NetShield configuration from the NetShield File Server Console.

To manage configuration files from the File Server Console:

1. Choose Configure NetShield NLM from the NetShield main menu.

   The NetShield NLM Configuration menu is displayed with the following options:

   - Configuration File Options
   - Configure Excluded Directories
   - NetShield Delay Factor
   - CRC Configuration Options
   - Password Configuration
   - Edit Cross Server Updating.

2. Choose Configuration File Options.

   The Configuration File Management Options menu is displayed with the following options:

   - Load Configuration Settings From File
   - Save Configuration Settings To File
   - Write Configuration Report To File
   - Print Current Configuration Settings

3. Choose Load Configuration Settings From File.

   Enter the configuration settings path and filename (SYS:\SYSTEM\VIR$CFG.DAT is the default)

4. Choose Save Configuration Settings To File.

   Enter the configuration settings path and filename (SYS:\SYSTEM\VIR$CFG.DAT is the default)

5. Choose Write Configuration Report to File.

   Enter the path and filename for the configuration report (SYS:\SYSTEM\VIR$CFG.RPT is the default)

6. Choose Print Current Configuration Settings.

   Select print queue from the list of available printers.

For more information about configuration files, refer to “Loading and Saving NetShield Configurations” in Chapter 3, “The NetShield Console.”

Configuring Excluded Directories

You can exclude specific directories from scanning from the NetShield File Server Console. You can exclude read-only directories from scanning to reduce scanning time, or “quarantine” directories that contain infected files already detected by NetShield.

To exclude directories from the File Server Console:

1. Choose Configure NetShield NLM from the NetShield main menu.

   The NetShield NLM Configuration menu is displayed with the following options:

   - Configuration File Options
   - Configure Excluded Directories
   - NetShield Delay Factor
   - CRC Configuration Options
   - Password Configuration
   - Edit Cross Server Updating

2. Choose Configure Excluded Directories.

   The Configure Excluded Directories menu is displayed with the following options:

   - Edit List of Excluded Directories
   - Apply Excluded List to All Scans

3. Choose Edit List of Excluded Directories

   The Currently Excluded Directories list is displayed. To add a directory, press INSERT and type the name of the directory and path.

4. Enable or disable Excluded Directories by toggling between the two choices.

   NOTE: NetShield will not exclude the selected directories unless Apply Excluded List to All Scans is enabled.

For more information about excluding directories, refer to “Excluding Directories” in Chapter 4, “Scanning.”

Setting the NetShield Delay Factor

The NetShield Delay Factor sets the amount of CPU time NetShield uses when performing a periodic scan.

NOTE: This setting can only be changed from the File Server Console.

There are ten levels of priority available, from 1 (the most CPU-intensive) to 10 (the least CPU-intensive). When NetShield is run with a priority setting of 1, 40 to 50 percent of CPU usage is added and approximately one file is scanned every second. When run with a priority of 10, 1 to 2 percent of CPU usage is added and one file is scanned approximately every 10 seconds. The default priority is 5.

To set the NetShield Delay Factor:

1. Choose Configure NetShield NLM from the NetShield main menu.

   The NetShield NLM Configuration menu is displayed with the following options:

   - Configuration File Options
   - Configure Excluded Directories
   - NetShield Delay Factor
   - CRC Configuration Options
   - Password Configuration
   - Edit Cross Server Updating.

2. Choose NetShield Delay Factor.

   Enter a number between 1 (the most CPU intensive) and 10 (the least CPU intensive). The default is 5.

CRC Configuration Options

CRC validation is a method for detecting new or unknown viruses. For more information about CRC validation, refer to “Cyclic Redundancy Check Validation” in Chapter 4, “Scanning.”

To configure CRC options from the File Server Console:

1. Choose Configure NetShield NLM from the NetShield main menu.

   The NetShield NLM Configuration menu is displayed with the following options:

   - Configuration File Options

- Configure Excluded Directories
- NetShield Delay Factor
- CRC Configuration Options
- Password Configuration
- Edit Cross Server Updating.

2. Choose CRC Configuration Options.

   The CRC Configuration Options menu is displayed with the following options:

   - Add CRC Code to External File
   - Verify CRC Code from External File
   - Remove CRC Code from External File
   - Edit External File Name

3. Create an external file of CRC codes by enabling Add CRC Code to External File. NetShield will create an external file of CRC codes the next time a scan is performed. Disable this option after your next scan or you will create a new CRC code external file every time you scan.
4. To perform CRC validation in subsequent scans (after the CRC external file has been created using the above procedure), enable Verify CRC Code from External File.
5. To create a new CRC external file (after upgrading software, for example), first delete the old file by enabling Remove CRC Code from External File. Then enable Add CRC Code to External File to CRC validation in subsequent scans (after the CRC external file has been created using the above procedure), enable Verify CRC Code from External File.
6. You can change the name of the external file by selecting Edit External File Name. (The default is vir$crc.dat)

For more information about CRC validation, refer to “Cyclic Redundancy Check Validation” in Chapter 4, “Scanning.”

Password Configuration

Enable password protection or change your NetShield password by choosing Password Configuration from the Configure NetShield NLM menu.

To configure your NetShield password from the File Server Console:

1. Choose Configure NetShield NLM from the NetShield main menu.

The NetShield NLM Configuration menu is displayed with the following options:

- Configuration File Options
- Configure Excluded Directories
- NetShield Delay Factor
- CRC Configuration Options
- Password Configuration
- Edit Cross Server Updating.

2. Choose Password Configuration.

   The Password Configuration menu is displayed with the following options:

   - Change Existing Password
   - Password Enable Status

3. Select Change Existing Password.

   Enter your current password (the default is **`netshield`**). Enter your new password, then confirm the change by entering the new password again.

4. Enable or disable password protection by toggling between the two choices.

NOTE: You will not have to use your password to access NetShield unless Password Enable Status is enabled.

Edit Cross Server Updating

You can allow or disallow cross server updating between servers through the NetShield File Server Console by selecting Edit Cross Server Updating from the NetShield NLM Configuration menu. Cross server updating allows servers to communicate information about virus signatures between each other. For more information about cross server updating, refer to “Cross Server Updating” in Chapter 4, “Scanning.”

To enable Cross Server Updating from the File Server Console:

1. Choose Configure NetShield NLM from the NetShield main menu.

   The NetShield NLM Configuration menu is displayed with the following options:

   - Configuration File Options
   - Configure Excluded Directories

- NetShield Delay Factor
- CRC Configuration Options
- Password Configuration
- Edit Cross Server Updating.

2. Choose Edit Cross Server Updating.

   The Edit Cross Server Updating menu is displayed with the following options:

   - Set Frequency of Updates
   - XServer Update Status

3. Enter the time (in minutes) between cross server updates.
4. Enable or disable Cross Server Updating by toggling between the two choices.

   NOTE: NetShield will not perform cross server updating unless XServer Update Status is enabled.

For more information about cross server updating, refer to “Cross Server Updating” in Chapter 4, “Scanning.”

Configuring Virus Reporting

NetShield can maintain a log of scanning events and virus detections.

To manage Virus Reporting from the File Server Console:

1. Choose Configure Virus Reporting from the NetShield main menu.

   The Virus Reporting Options menu is displayed with the following options:

   - Configure Log File Settings
   - Select Log File Reports

2. Choose Configure Log File Settings.

   The Log File Configuration Options menu is displayed with the following options:

   - Enter Log File Path
   - Enable/Disable Logging to File

3. Choose Enter Log File Path and enter a path in the provided box or choose INSERT to locate a path.

4. Enable or disable logging to file by toggling between the two choices.

   NOTE: NetShield will not maintain scan result logs if Logging to File is not enabled.

   Hit ESCAPE to return to the Virus Reporting Options menu.

5. Choose Select Log File Reports.

   The Log File Reports menu is displayed with the following options:

   - View Contents of Log File
   - Print Contents of Log File

   You can view or print the contents of the log file to observe scanning results.

For more information about logging, refer to “Logging” in Chapter 5, “Notification and Reporting.”

Configuring Network Security

For highly secure networks, NetShield can detect and log any attempts to write to read-only directories. In addition, you can also suspend read-only protection for authorized users to make changes to monitored directories. Refer to Chapter 6, “Security,” for more information.

Enabling Network Security Configuration

To enable the Network Security menu:

1. Choose Network Security from the NetShield Main menu.

   The Enter Password to Enable Network Security Configuration menu is displayed.

2. Enter the password in the provided box.

   NOTE: The default password is: `login admin`

   The Configure Network Security menu is displayed with the following options:

   - Edit Network Security Configuration
   - Set Path for Log File
   - Save Current Configuration to a File
   - Restore Current Configuration From a File
   - Current Network Security Status

3. Enable or disable Network Security by toggling between the two choices.

   NOTE: Your NetShield security choices will not be implemented until Current Network Security Status is set to enabled.

Edit Network Security Configuration

To edit Network Security Configuration from the File Server Console:

1. Choose Edit Network Security Configuration from the Network Security menu.

   The Edit Network Security Configuration menu is displayed with the following options:

   - Create File and Extension Master List
   - Select Entries to Monitor from Master List

- Select Files to be Excluded from Monitoring
- Select Directories to Monitor for All Users
- Change Monitored Users
- Change Temporary Authorization
- Change Network Security Password

2. Choose Create File and Extension Master List to create a master list of the files and/or file extensions, such as all executable files (COM, EXE, SYS, BIN, OVL, DLL) that you want to monitor.

   Press INSERT and select the volume you want to monitor files from. Create a master list using the ENTER and DELETE keys.

   NOTE: To monitor these files, you will have to add them to another list (see below).

3. Choose Select Entries to Monitor from Master List to limit scans to specific files or file extensions, such as all executable files (COM, EXE, SYS, BIN, OVL, DLL).

   Add files to the Entries to Monitor list by pressing ENTER. Remove files you no longer with to monitor by pressing DELETE. To add or remove files from the master list, refer to Create File and Extension Master List (see above).

4. Choose Select Files to be Excluded from Monitoring to exclude specific files from monitoring, such as a backup file or a data file.

   Press INSERT and select the volume you want to ignore files from. Add or remove files from the list using the ENTER and DELETE keys.

5. Choose Monitor for All Users to monitor all write access to selected directories by choosing Monitor for All Users.

   Press INSERT and select a volume. Add or remove directories from the list using the ENTER and DELETE keys.

6. Choose Change Monitored Users to restrict write access to specific users.

   Press INSERT to select from a list of users. Add or remove users from the Monitored Users list using the ENTER and DELETE keys.

7. Choose Change Temporary Authorization to authorize one or more users to write to Monitor for All Users-protected directories, so they can perform software upgrades, installs, etc.

   Press INSERT to select from a list of users. Add or remove users from the Temporary Authorization list using the ENTER and DELETE keys.

Enter the Enable Administration Access time, in minutes. This time must be set to at least 1 minute. The Access Will Remain For field indicates how much time is remaining for this user.

NOTE: If the administrative access time runs out while changes are being made to monitored directories, NetShield competes the current write operation, if any, then prevents additional changes.

8. Choose Change Network Security Password to change your security password.

   Enter your current password (the default is **`login admin`**). Enter your new password, then confirm the change by entering the new password again.

For more information, refer to Chapter 6, “Security.”

Security Log File Options

To manage the Security Log File:

1. Choose Set Path for Log File from the Network Security menu.

   Enter the path for the log file (SYS:\SYSTEM\NETSHLD.LOG is the default). Selecting overwrite will save this log over the existing log file; selecting append will add this log to the end of the existing log file.

Security Configuration Options

To load or save a Security configuration file:

1. Choose Save Current Configuration to a File from the Network Security menu.

   Enter the path for the log file (SYS:\SYSTEM\NETSHLD.DAT is the default).

2. Choose Restore Current Configuration from a File to load a previously saved security configuration.

   Enter the path for the log file (SYS:\SYSTEM\NETSHLD.DAT is the default).

Appendix A Troubleshooting NetShield

If you are having a problem with NetShield, refer to the commonly-asked questions and error messages listed below. For more help, refer to “How Do I...?” in the On-Line Help or to “McAfee Support” in Chapter 1, “Introducing NetShield.”

Error Messages

Unknown Error Number

NetShield reported an unknown error. Verify that the server you are attempting to administer is running NetShield version 2.2 or greater.

General System Error

An internal error occured. If this error persists, exit and restart NetShield. If it continues, contact Customer Support.

Invalid Function Argument

Incorrect or invalid information was presented to NetShield. Verify the information, and try the operation again.

Internal System Error

An internal error occured. If this error persists, exit and restart NetShield. If it continues, contact Customer Support at (408) 988-3832, or refer to “McAfee Support” in Chapter 1, “Introducing NetShield.”

Insufficient Data Error

Insufficient data was provided. Verify that all required fields are filled in, and try the operation again.

Unable to Attach to Server

You may have reached your maximum allowable connections under Novell. Terminate an existing connection and try again.

No Such File or Directory

The selected file or directory does not exist. Select a valid file or directory.

Data Corruption Error

The input data is corrupted. Try the operation again.

Data Corruption Error

The response from the server was corrupted. Try the operation again.

Invalid Password Error

The password provided does not match the password required by the fileserver. Verify that you have the correct password and try again.

Insufficient Memory to Run WSCAN

The system reported insufficient memory to run WSCAN.

“WSCAN=” Entry Not Found in WIN.INI File

Ensure the section [VIRUSSCAN] exists in WIN.INI and it contains the correct file name and path.

Improper Time Format

Time must be non-zero and be in the following format: xx:xx. Note that NetShield uses 24-hour time (00:01 to 24:00).

Improper Date Entered

For Monthly Periodic Scanning, the date must be between 1 and 31, inclusive.

Invalid Settings for MHS Server

There must be entries for Novell Global Message Handling System (GMHS) Server name, Mail Directory and User Name.

Error Connecting to MHS Server

NetShield was unable to connect to Novell Global Message Handling System (GMHS) Server. Verify server name, mail directory, user name and password are correct.

No Log File Entered

Netshield needs a path and file name to store the log information.

New Password Mismatch Error

The new passwords entered do not match each other. Please try again.

Scan in Progress Error

A scan is in progress. Some settings will not take effect until all current scans are terminated and restarted.

Data Send Error

An error occurred sending data to the server. Verify that the connection is still valid and retry the operation.

Data Receive Error

An error occurred receiving data from the server. Verify that the data is still valid, and retry the operation.

The Operation Timed Out

The operation timed out waiting for a response. Verify that the connection is valid, the server is operational, and the server is running NetShield, and try the operation again.

No Volume Selected

No volume was selected for scanning. Choose from the list of available volumes or cancel the operation.

WSCAN Not Found

WSCAN.EXE not found. Check Path and Filename in WIN.INI [VIRUSSCAN] Section.

Duplicate Entry

An entry that already exists was specified to be added.

NetShield Questions

Q: How many passwords does NetShield have?

A: There are two passwords used by NetShield. The NetShield password allows you to attach to a server (the default for this password is **`netshield`**). The NetLock password enables the security menu (the default for this password is **`login admin`**). Both passwords are case insensitive. Refer to “Changing Your Password” in Chapter 3, “The NetShield Console.”

Q: Does NetShield alert all users on the contact list?

A: Yes. If the Minimum Message Interval option is being used, however, NetShield only sends one message per X minutes. Refer to “Enabling Mail Notification” in Chapter 5, “Notification and Reporting.”

Q: I receive an OAS monitor hook installation failure message when I try to enable On Access Scanning.

A: Down the server and update the CLIB.NLM to the latest version (use LIBUP4.EXE). Refer to “Novell NetWare 3.11 and 3.12 File Server Requirements” in Chapter 2, “Installation.”

Q: I configured NetLock Security but none of my choices have gone into effect.

A: Make sure you have selected the Enable NetLock Security check box in the Security | Settings dialog box. Refer to “Selecting Security Settings” in Chapter 6, “Security.”

Q: I added users to the User Notification List but they are not appearing on the Notification property page.

A: Make sure you have selected the Enable User Notification check box in the Notification | User dialog box. Refer to “Enabling User Notification” in Chapter 5, “Notification and Reporting.”

Q: I added files to the Monitoring Master List but they are not being monitored.

A: You must add them to another list. See “Creating a Master List” and “Selecting From Master List” in Chapter 6, “Security.”

File Server Questions

Q: What are AIO and AIOCOMX and why do I need them?

A: AIO.NLM is an asynchronous I/O library required for NetShield. AIOCOMX.NLM is an asynchronous I/O driver required to implement pager support. These patches are supplied with the CD ROM release and are also available through Novell and McAfee. Refer to “Novell NetWare 3.11 and 3.12 File Server Requirements” in Chapter 2, “Installation,” and “Pager Notification” in Chapter 5, “Notification and Reporting.”

Q1: I receive an OAS monitor hook installation failure message when I try to enable On Access Scanning.

Q2: I receive “Loader cannot find public symbol...” addresses when I try to load NetShield at the File Server Console prompt.

A: Down the server and update the CLIB.NLM to the latest version (use LIBUP4.EXE). Refer to “Novell NetWare 3.11 and 3.12 File Server Requirements” in Chapter 2, “Installation.”

Q: My server abends when I load NetShield.

A: Either move NetShield and its data files to the SYS\SYSTEM subdirectory, or add a SEARCH ADD to the AUTOEXEC.NCF or NETSHLD.NCF to the directory where NetShield is stored. This is caused by a bug in NWSNUT.NLM, supplied by Novell. Refer to Chapter 2, “Installation.”

Q: I load NetShield at the File Server Console prompt and it starts to load, but then returns me to the File Server Console prompt.

A: NetShield data files, SCAN.DAT and NAMES.DAT, are either missing, damaged or marked “Read Only.” Ensure that they are in the same directory as the NLM and are not marked “Read Only.” Refer to Chapter 2, “Installation.”

Q: What directory should I put the NetShield NLM in?

A: McAfee recommends SYS\SYSTEM. If you choose to put it in another directory, you **must** add a SEARCH ADD statement to the AUTOEXEC.NCF or execute it at the console before loading NetShield. Refer to Chapter 2, “Installation.”

Q: When I unload NetShield I receive short term memory allocation errors.

A: Make sure you have SPXS.NLM loaded. It is available from all of McAfee’s electronic sites in a Novell-supplied patch file called STRTL3.EXE. Refer to “McAfee Support” in Chapter 1, “Introducing NetShield.”

Q: What is the precise order for loading the NLMs?

A: There is no required order other than ensuring that any patches (SPXS, SPXFIX2, etc.) are loaded before NetShield. We also recommend loading NetShield before any backup software. Refer to “Loading NLMs” in Chapter 2, “Installation.”

Q: Why do I need to down the server after loading patches?

A: To ensure that the patches load properly. Refer to “Novell NetWare 3.11 and 3.12 File Server Requirements” in Chapter 2, “Installation.”

Appendix B Additional References

The McAfee BBS and CompuServe McAfee Virus Help Forum are excellent sources of information on virus protection. Batch files and utilities to help you use VirusScan software are often available, along with helpful advice.

Independent publishers, colleges, training centers, and vendors also offer information and training about virus protection and computer security.

We especially recommend the following publications:

- Ferbrache, David. *A Pathology of Computer Viruses*. London: Springer-Verlag, 1992. (ISBN 0-387-19610-2)
- Hoffman, Lance J. *Rogue Programs: Viruses, Worms, and Trojan Horses*. Van Nostrand Reinhold, 1990. (ISBN 0-442-00454-0)
- Jacobson, Robert V. *The PC Virus Control Handbook,* 2nd Ed. San Francisco: Miller Freeman Publications, 1990. (ISBN 0-87930-194-0)
- Jacobson, Robert V. *Using McAfee Associates Software for Safe Computing*. New York: International Security Technology, 1992. (ISBN 0-9627374-1-0)

In addition, the following sources can provide useful information about viruses:

- National Computer Security Association (NCSA), 10 South Courthouse Avenue, Carlisle, PA 17013
- CompuServe McAfee Virus Help Forum **GO MCAFEE**
- Internet **`comp.virus`**newsgroup
- FTP site: ftp.mcafee.com
- America On Line **`MCAFEE`**
- McAfee BBS: (408) 988-4004

  1200 bps to 28,800 bps

  8 bits, no parity, 1 stop bit

  24 hours, 365 days a year

Index